POLITÉCNICA
"Ingeniamos el futuro"

CAMPUS
DE EXCELENCIA
INTERNACIONAL

2012

CURSOS DE VERANO de la Universidad Politécnica de Madrid

PATROCINAN

Santander

Canal de Isabel II

ECOEMBES

FUNDACION ACS

AMETIC

109 **SEGURIDAD FÍSICA EN SISTEMAS EMPOTRADOS: UNA ASIGNATURA PENDIENTE** *(11 y 12).*

Director: Jose Manuel Moya Fernández

CeDInt POLITÉCNICA

12:30 a 14:30	**Cracking y ataques físicos sobre dispositivos electrónicos** Vicente Jara, Investigador del Centro de Domótica Integral (CEDINT), Universidad Politécnica de Madrid

GB2S group of biometrics biosignals and security

¿DE QUÉ VAMOS A HABLAR?

-El tema se ha introducido ya.
-Entramos en materia.

-Hay que explicar muchas cosas y tomaremos muchos datos de especialidades diversas.
-No todo se va a entender, pero es suficiente seguir el hilo.

-"Cracking"
-"Ataques"
-"Físicos"
-"Dispositivos"
-"Electrónicos"

¿DE QUÉ VAMOS A HABLAR?

-Hasta los agujeros negros dejan evidencia de su existencia.

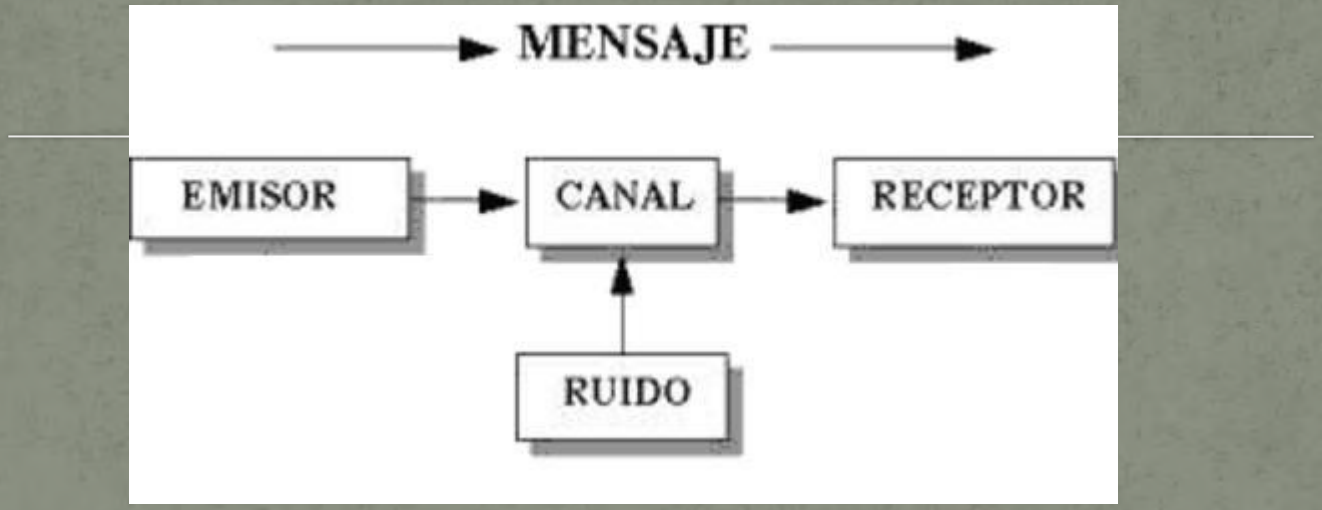
-“Posiblemente” cualquier sistema siempre haya de contar con “dejar rastros”, o “dejar evidencia”.
-Relaciones entre magnitudes físicas y químicas.

¿DE QUÉ VAMOS A HABLAR?

-Dispositivos electrónicos.

¿DE QUÉ VAMOS A HABLAR?

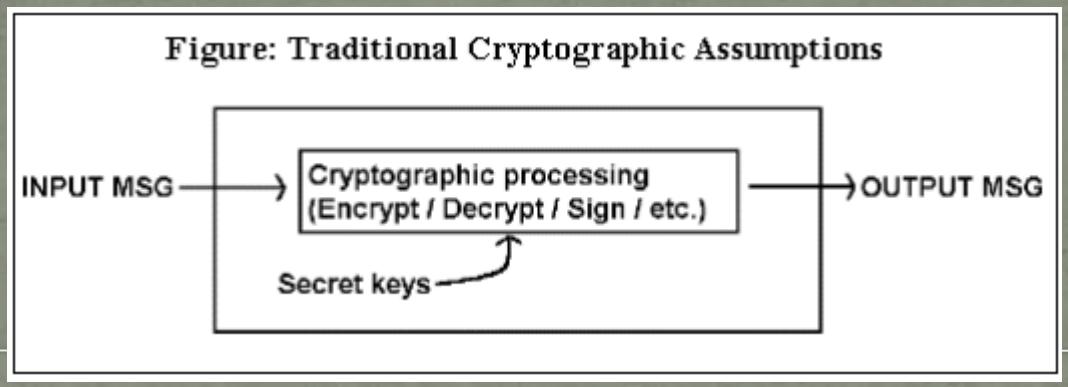
-No obstante, nos centramos preferentemente en este esquema, que aún sigue siendo muy general.
-Internet de las cosas.



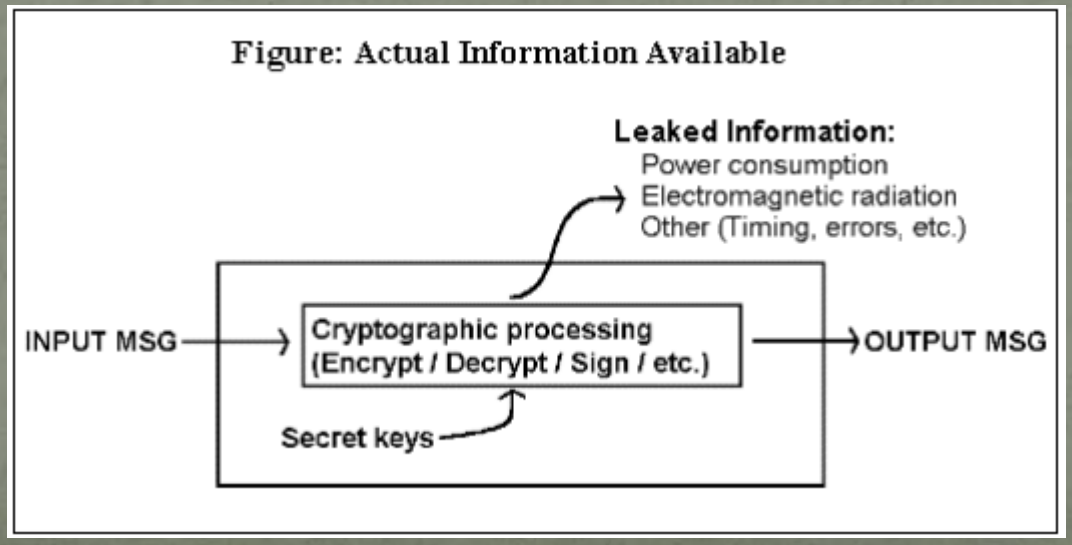
¿DE QUÉ VAMOS A HABLAR?

-Y lo veremos de esta otra forma, o mejor, de dos formas.

(a)



(b)



¿DE QUÉ VAMOS A HABLAR?

-Un referente moderno: Paul Carl Kocher (1973-), EE.UU.

"*Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems*" (1996)

MAESTRO CONTRA DISCÍPULO: PLATÓN VS. ARISTÓTELES

-Rompiendo algoritmos criptográficos

(a) Atacando los algoritmos,
sus propiedades matemáticas.
El mundo platónico de las Ideas es invariante.

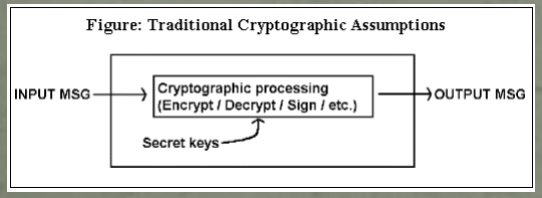
(b) Atacando las implementaciones
de los algoritmos, la física-química.
No hay más mundo que éste, el "en sí" está
en la abstracción de los particulares.

+Como no se puede entender Aristóteles sin pasar por la Academia, antes del Liceo veamos qué dice Platón (criptoanálisis).

CRIPTOANÁLISIS

-Rompiendo algoritmos criptográficos

Empecemos por la (a).....



CIFRADO POR SUSTITUCIÓN

I-"Viaje al centro de la Tierra". Julio Verne (1864)

"In Sneffels Joculis craterem quem delibat Umbra Scartaris Julii intra calendas descende, Audax viator, et terrestre centrum attinges. Quod feci, Arne Saknussemm"

("Desciende el cráter del volcán de Sneffels cuando la sombra de Scartaris llega a acariciarlo antes de las calendas de julio, audaz viajero, y llegarás al centro de la Tierra. Así lo hizo, Arne Saknussmm").

CRIPTOANÁLISIS

-Rompiendo algoritmos criptográficos

Empecemos por la (a)…..
…pero nunca….
sobrestimemos a un genio.

¡Hagámoslo nosotros!

CIFRADO POR SUSTITUCIÓN

I-"Viaje al centro de la Tierra". Julio Verne (1864)

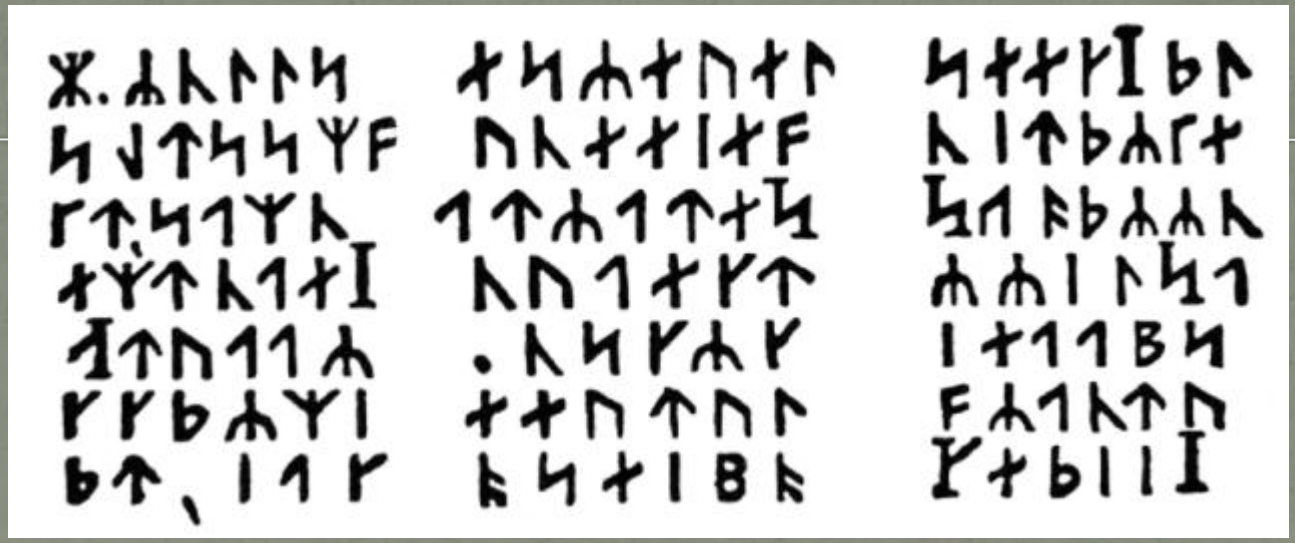
"In Sneffels Joculis craterem quem delibat Umbra Scartaris Julii intra calendas descende, Audax viator, et terrestre centrum attinges. Quod feci, Arne Saknussemm"

("Desciende el cráter del volcán de Sneffels cuando la sombra de Scartaris llega a acariciarlo antes de las calendas de julio, audaz viajero, y llegarás al centro de la Tierra. Así lo hizo, Arne Saknussmm").

Estamos en la Universidad

-Leamos a Julio Verne como adultos….. ¿qué es esto?

+Julio Verne escribía para jóvenes pero también para adultos, no lo olvidemos.



Algunos datos curiosos:

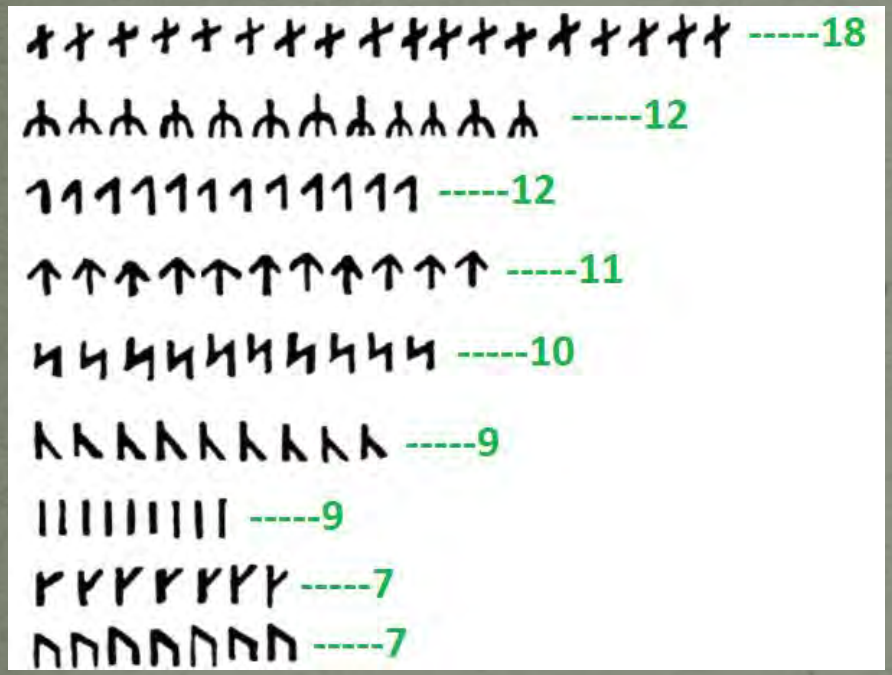
-Signos "inesperados", como el punto (".") y la coma (","):

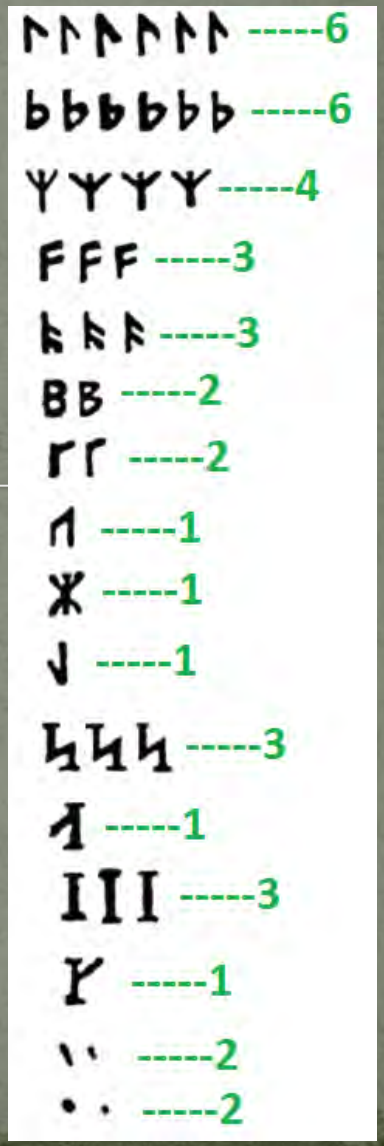
+No es algo normal en criptografía, pues se eliminan al cifrarlos.
Y eso si es que mantienen el sentido de punto y coma, o los alteran (hipótesis).

-Hay algunos **signos que se parecen a otros, casi iguales**:

+**Hipótesis**: Es como si fueran letras mayúsculas, de los de la izquierda (más numerosos).

-¿Qué signos aparecen?
-Frecuencia de aparición.

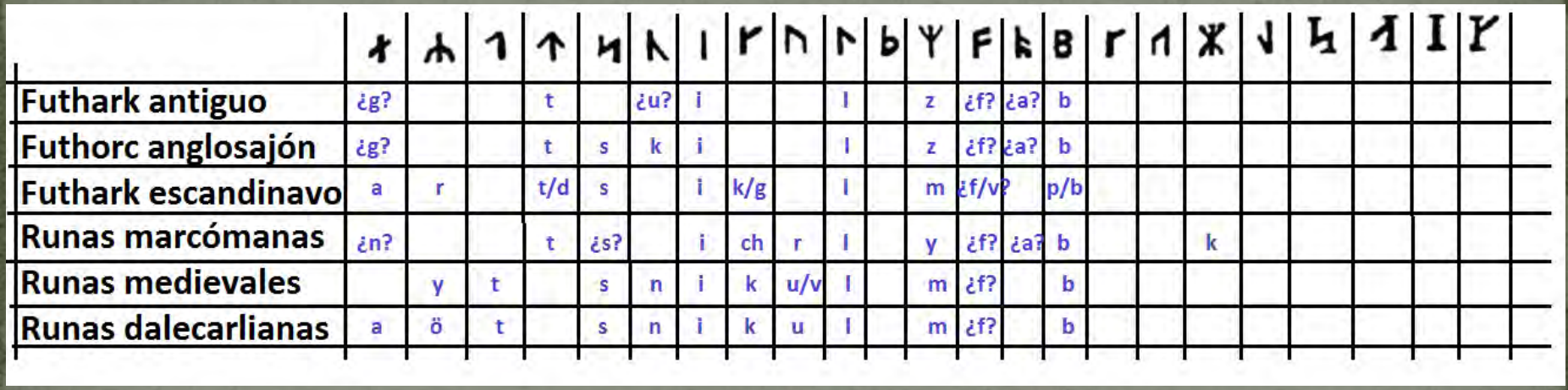




-Lingüística antigua (runas escandinavas, islandesas y bretonas):

Tomando las runas más parecidas a las de nuestro criptograma tenemos que movernos entre el Futhark antiguo, el Futhorc anglosajón, el Futhark escandinavo, las runas marcómanas, las medievales y las dalecarlianas, no siempre iguales en sus grafías.

Y lo que vemos es sorprendente:



Futhark antiguo	¿g?			t		¿u?	i			l		z	¿f?	¿a?	b							
Futhorc anglosajón	¿g?			t	s	k	i			l		z	¿f?	¿a?	b							
Futhark escandinavo	a	r		t/d	s		i	k/g		l		m	¿f/v?		p/b							
Runas marcómanas	¿n?			t	¿s?		i	ch	r	l		y	¿f?	¿a?	b			k				
Runas medievales		y	t		s	n	i	k	u/v	l		m	¿f?		b							
Runas dalecarlianas	a	ö	t		s	n	i	k	u	l		m	¿f?		b							

+**Conclusión**: Julio Verne ha inventado los signos, en base a la grafía de las runas.

+ **Hipótesis**: El hecho de contar 23 signos más dos posibles de puntuación, que podrían hacer 25 elementos distintos, hace pensar en el posible alfabeto actual de 26 letras, sin contar la “ñ” española:

{a,b,c,d,e,f,g,h,i,j,k,l,m,n,o,p,q,r,s,t,u,v,w,x,y,z}.

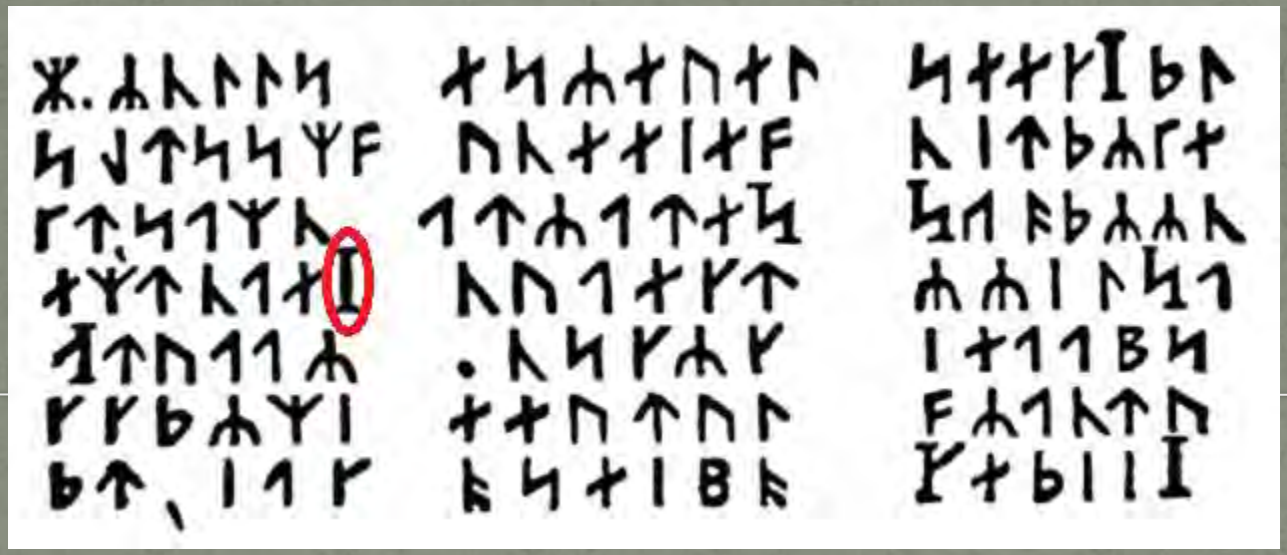
+ **Hipótesis**: No obstante, pensando en que sí hay dos signos de puntuación, y alguna letra mayúscula, por el fuerte parecido, nos hace pensar en un alfabeto menor, no tan desarrollado (sin “w”, quizás), o al menos sin presencia de todas las letras en el criptograma.

-Parece que hay un modo de ordenarse.

7 elementos	7 elementos	7 elementos
7 elementos	7 elementos	7 elementos
7 elementos	7 elementos	7 elementos
7 elementos	6 elementos	6 elementos
6 elementos	6 elementos	6 elementos
6 elementos	6 elementos	6 elementos
6 elementos	6 elementos	6 elementos

+ Conclusión: Una estructura de este modo ya nos indica que posiblemente se mueva en sentido horizontal y de arriba hacia abajo.
+ Conclusión: Y además coloque un elemento tras otro en cada sub-bloque.

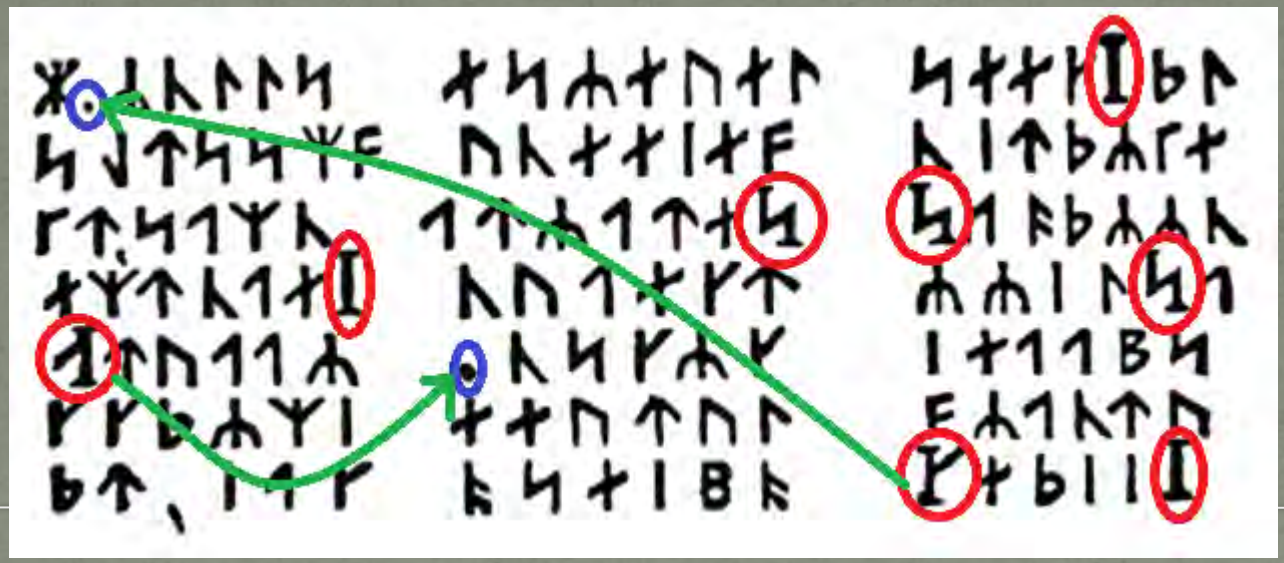
+Y eso significaría que podemos decir que el **último elemento** en colocarse es:



+Pero este signo es de los que suponíamos que podía ser una mayúscula.
¿Pero podría acabar con mayúscula?
Hipótesis: Sí, puede ser si es una inicial de un nombre.

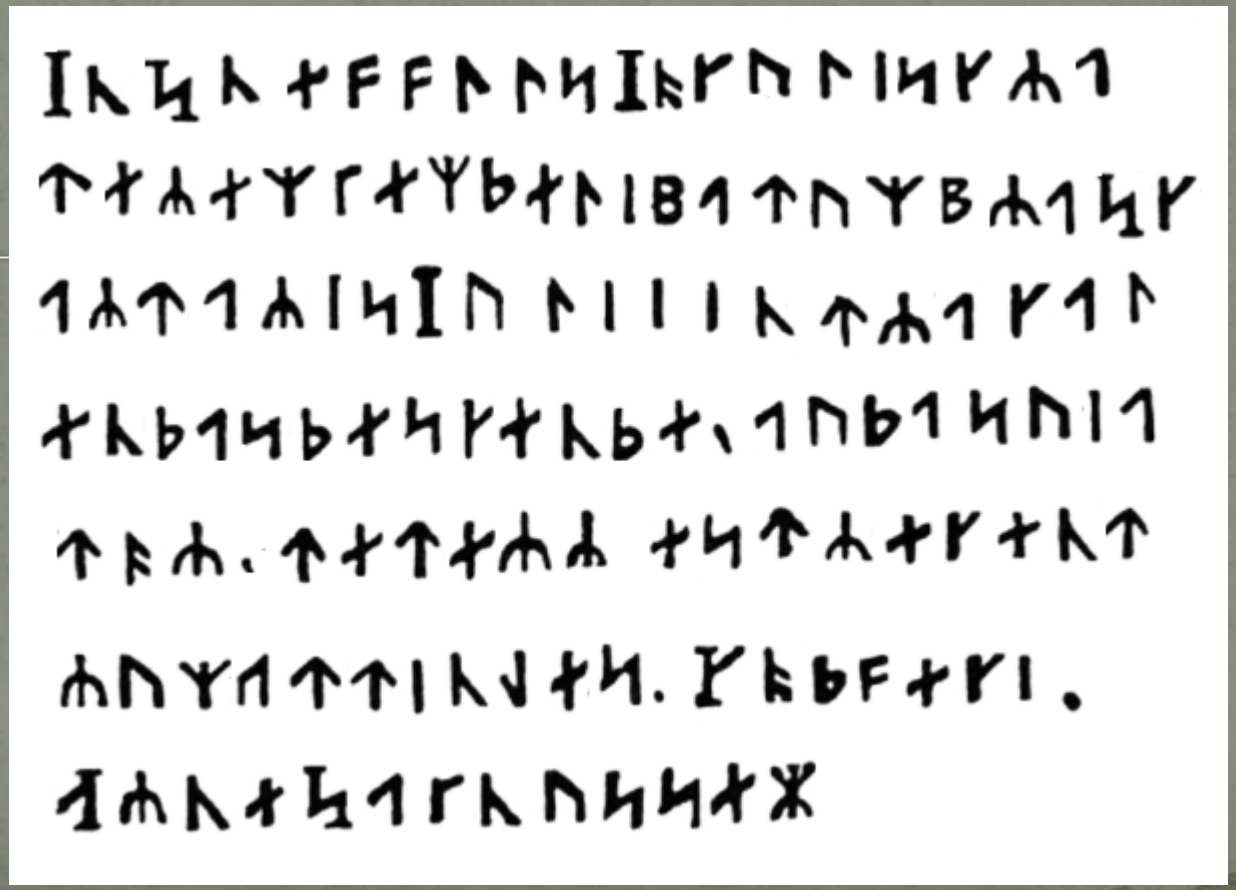
+ **Hipótesis**: Otra opción es que sea realmente el inicio del texto.

+Estudiemos los puntos (“.”).



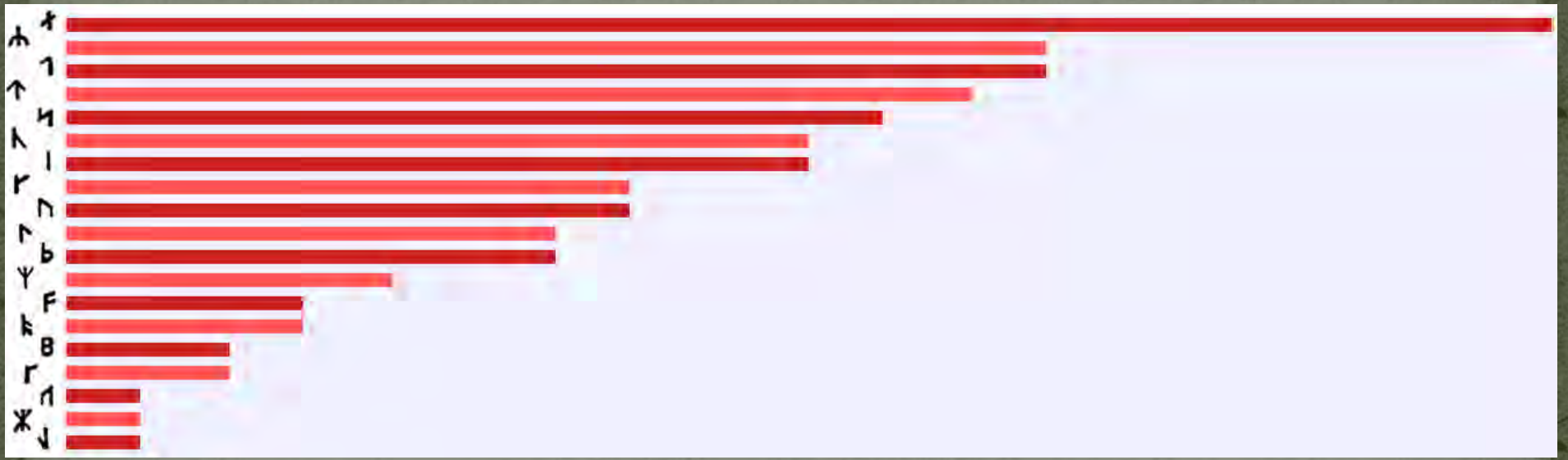
+ <u>Conclusión</u>: Algunos signos que pensábamos que eran mayúsculas no lo parecen ser, pero dos de ellos sí resultan ser y nos indican el sentido de escritura, que es precisamente inverso (primero el punto ".", y luego la mayúscula).

- ¿Qué tenemos?



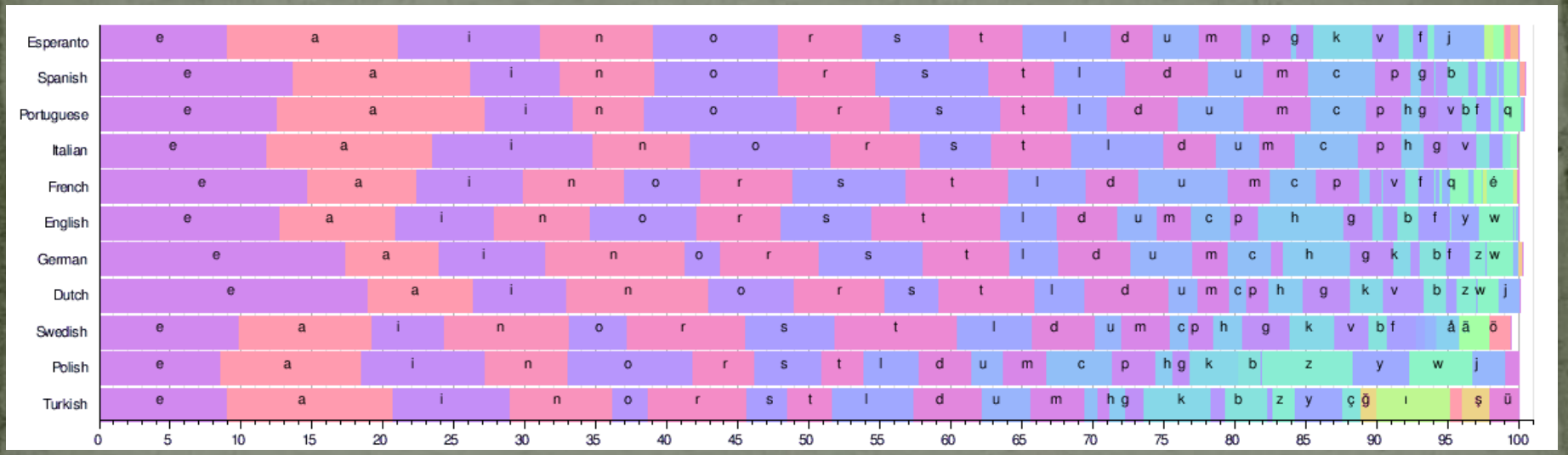
-Más estudio de frecuencias:

Volvamos a las frecuencias, y veamos qué tenemos:
(Como parece que hay mayúsculas, y quizá haya puntos y comas, sólo haremos el análisis de frecuencias para los primeros 19 signos ; quitamos los 6 últimos).

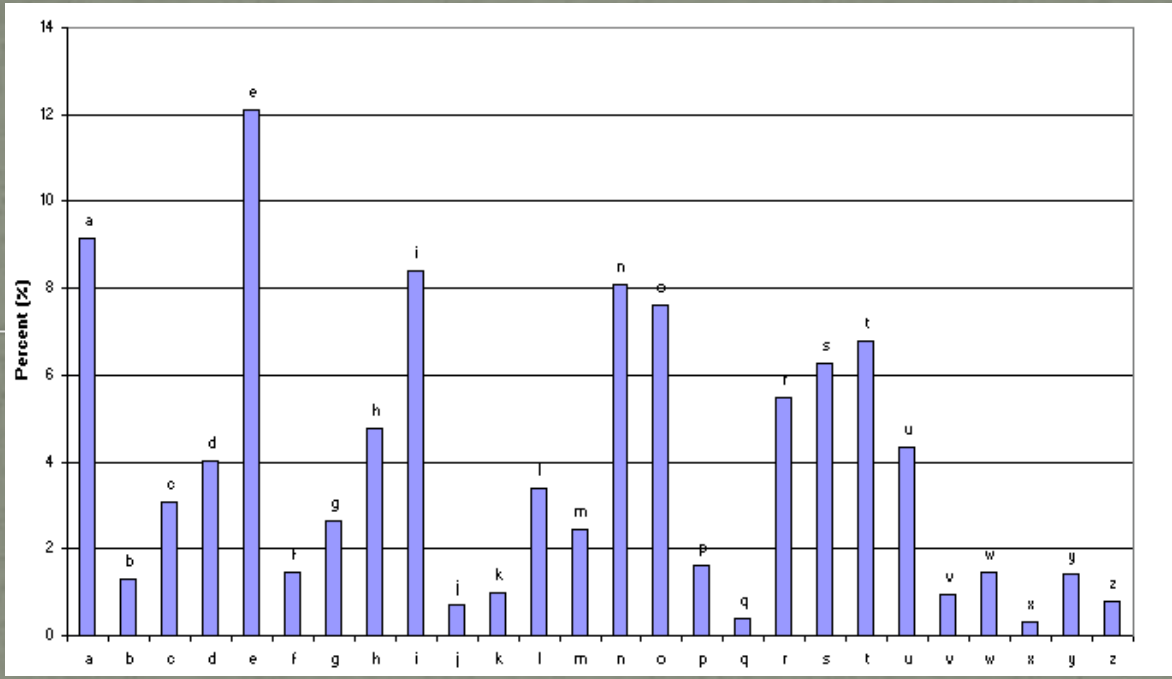


-¿En qué idioma?

Haciendo un análisis de frecuencias con posibles idiomas (cosa que no haremos, hay que usar el índice de coincidencia (IC), un estudio de bigramas y quizás trigramas, y un análisis de posibles vocales y consonantes, llegamos a nuestro idioma, que resulta ser…..):

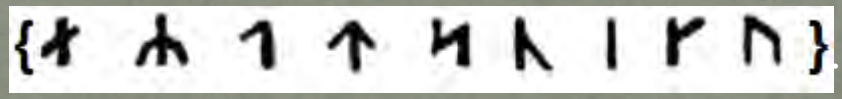


+ **Hipótesis**: Una muy posible opción es que sea **latín**:



- **Algunas sustituciones posibles:**

Considerando las frecuencias de los signos más frecuentes en nuestro criptograma y en el latín, haríamos los siguientes cambios, como hipótesis muy posibles, con los 8 primeros caracteres más repetidos:

{e,a,i,n,o,t,s,r}, como 

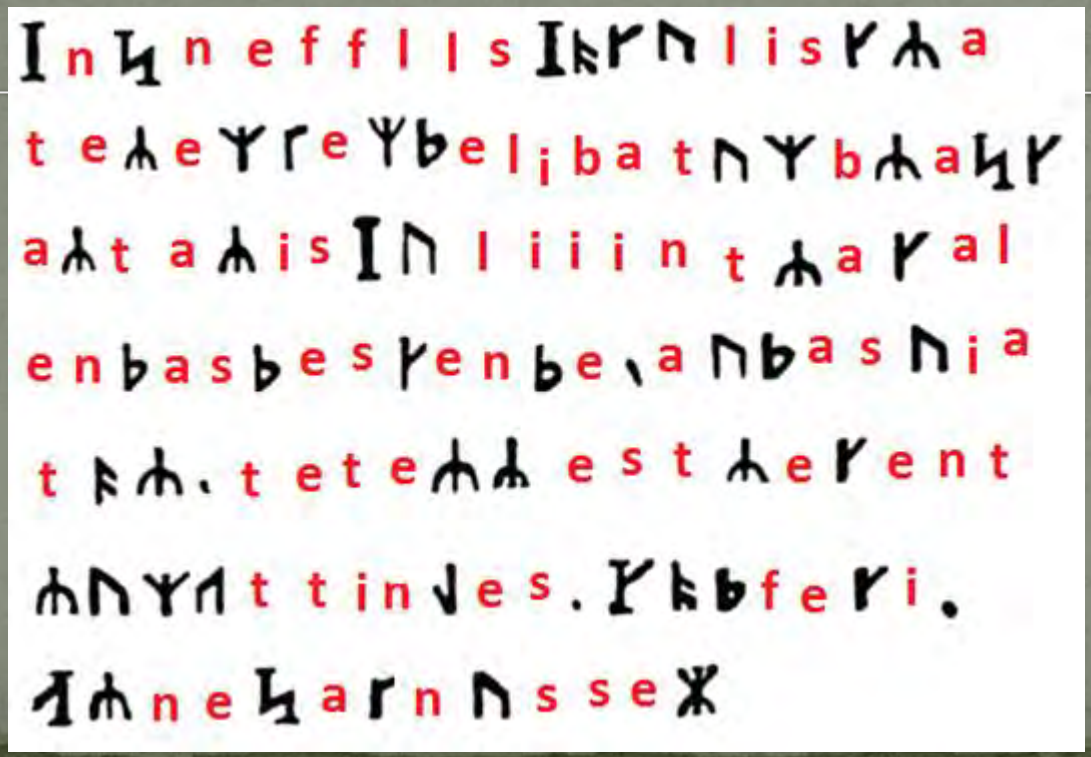
Esto nos lleva a suponer junto con la tabla:

																																		
Futhark antiguo	¿g?			t		¿u?	i			l		z	¿f?	¿a?	b															
Futhorc anglosajón	¿g?			t	s	k	i			l		z	¿f?	¿a?	b															
Futhark escandinavo	a	r		t/d	s		i	k/g		l		m	¿f/v?		p/b															
Runas marcómanas	¿n?			t	¿s?		i	ch	r	l		y	¿f?	¿a?	b			k												
Runas medievales		y	t		s	n	i	k	u/v	l		m	¿f?		b															
Runas dalecarlianas	a	ö	t		s	n	i	k	u	l		m	¿f?		b															

+Hipótesis

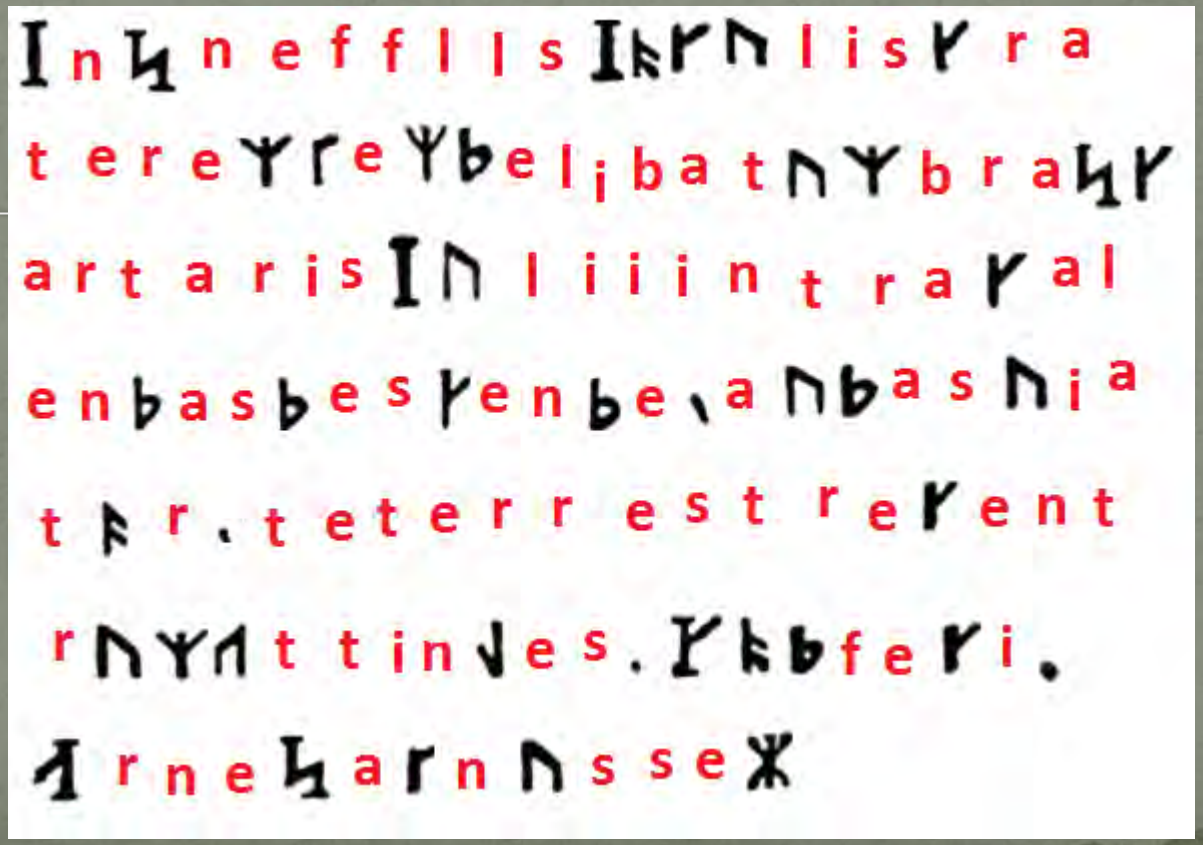
(mostraremos sólo –por rapidez- el caso correcto de la letra “a”, que es la segunda de las opciones; haciendo las dos veríamos con cuál quedarnos).

+Y además siguiendo el posible sentido de las runas, y los porcentajes de frecuencias entre los signos rúnicos y el latín, podemos suponer:

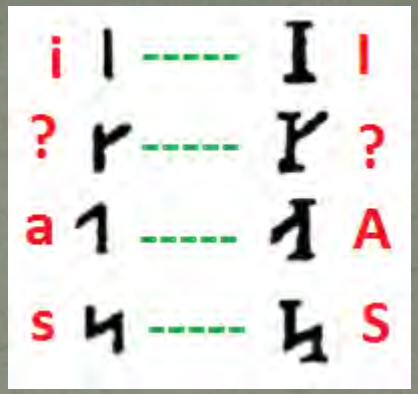


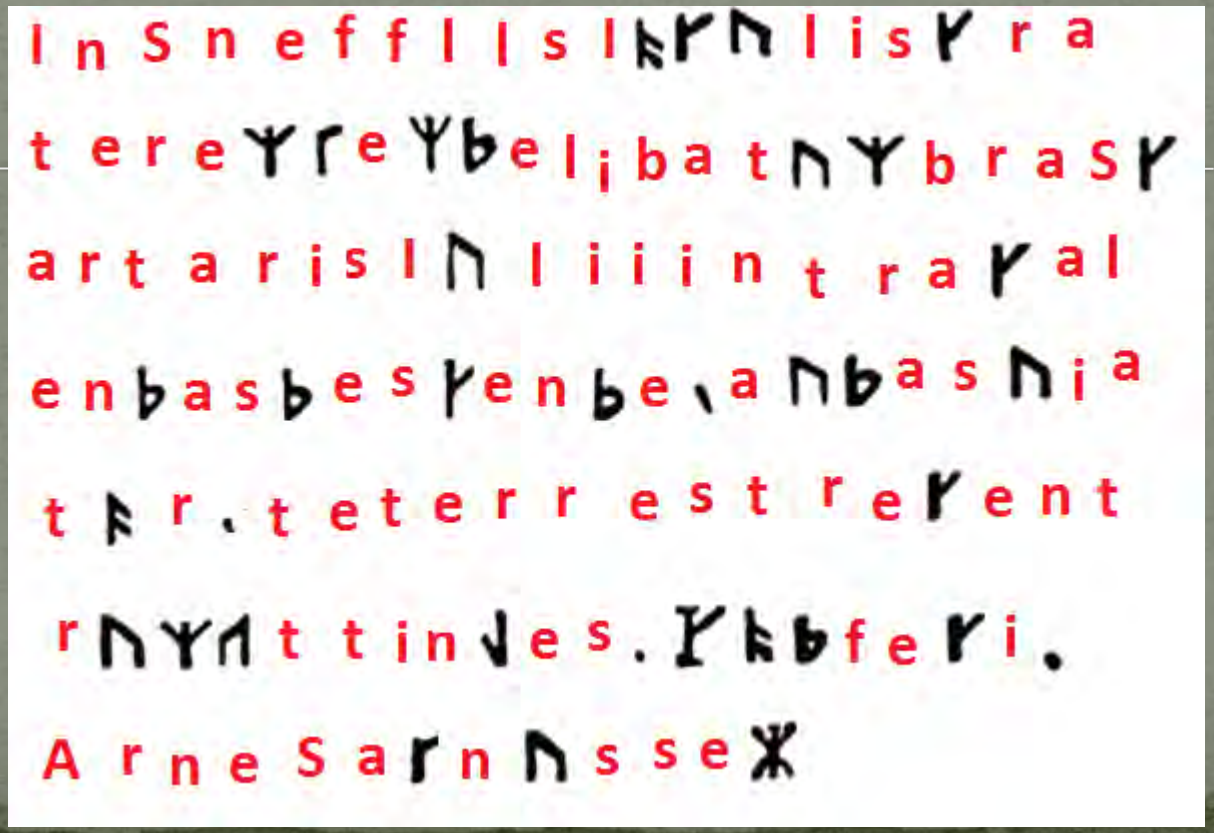
- Más suposiciones:

Ante la situación mostrada, para el signo 2º más probable,  , si es vocal o consonante, viendo las más probables en el latín, queda claro que es una consonante, luego supondremos que es la "r".



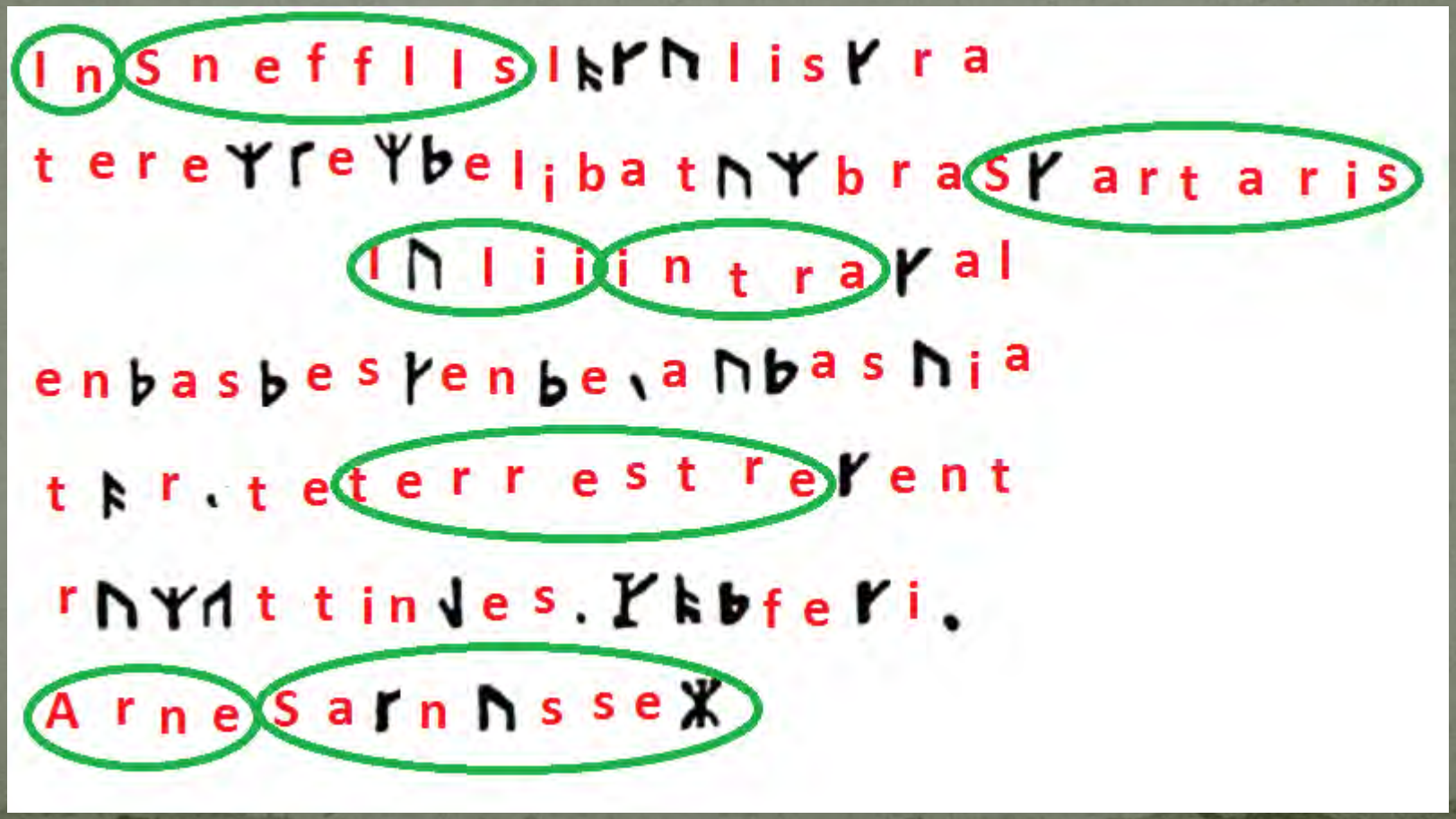
- Usando ahora la hipótesis de las mayúsculas:





-Echemos un ojo al texto intentando **localizar palabras**:

Agrupando algunas palabras que se ven y otras por las mayúsculas marcadas, tenemos:



+Viendo las letras que nos quedan….., y el texto anterior, podemos decir:

Quedan del alfabeto de 26 letras: {c,d,g,h,j,k,m,o,p,q,u,v,w,x,y,z}.

+Hilando algo más fino con las frecuencias latinas:

Las 10 primeras letras de las obras de

(a: nuestro texto previo): {e,a,i,n,o,t,s,r,h,u}
(b) Julio César: {e,i,t,u,a,s,r,n,o,m}
(c) Séneca: {i,e,t,u,a,s,n,m,o,r}
(d) Tito Livio: {e,i,u,a,s,r,n,m,o,c}

Echamos en falta
(a) {o,h,u}
(b) {u,o,m}
(c) {u,m,o}
(d) {u,m,o,c}

+Hilando algo más fino con las frecuencias latinas:

Las 10 primeras letras de las obras de

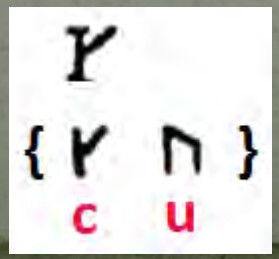
(a: nuestro texto previo): {e,a,i,n,o,t,s,r,h,u}
(b) Julio César: {e,i,t,u,a,s,r,n,o,m}
(c) Séneca: {i,e,t,u,a,s,n,m,o,r}
(d) Tito Livio: {e,i,u,a,s,r,n,m,o,c}

Echamos en falta

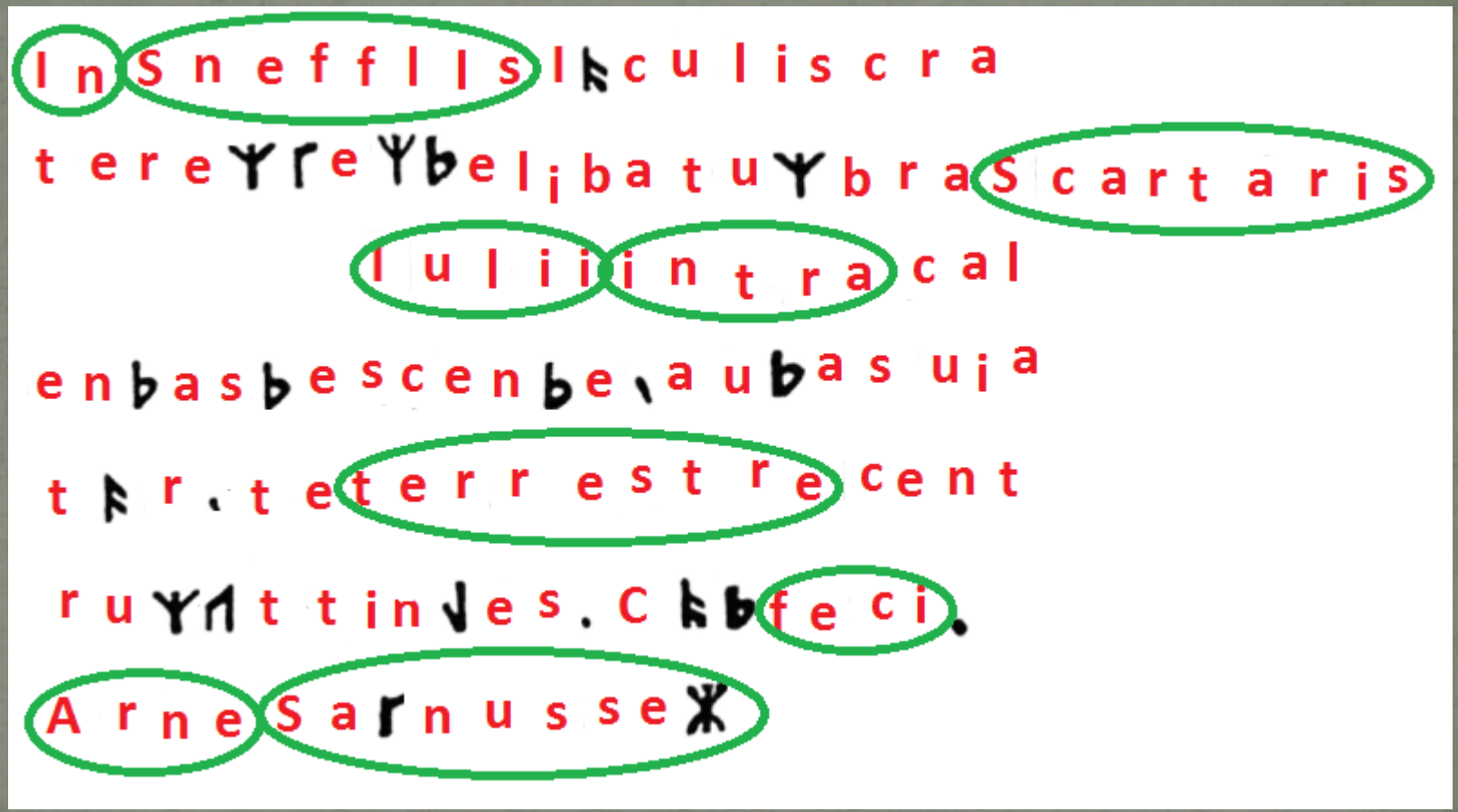
(a) {o,h,u}
(b) {u,o,m}
(c) {u,m,o}
(d) {u,m,o,c}

Luego sobre  aplicamos las posibilidades de ser {o,h,u,m,c}, que son $V_{5,2}$=20 posibilidades.

Lo cual da como mejor opción:



- Por ahora:

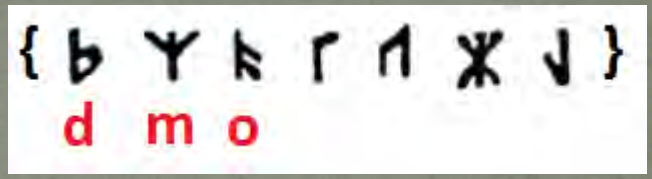

In Sneffl s lh culiscra
tereYreYbel¡batuYbraScartaris
lulii intra cal
enbasbescenbe,aubasua
th r.teterrestrecent
ruYntt tinJes.Chbfeci.
Arne Sarnusse

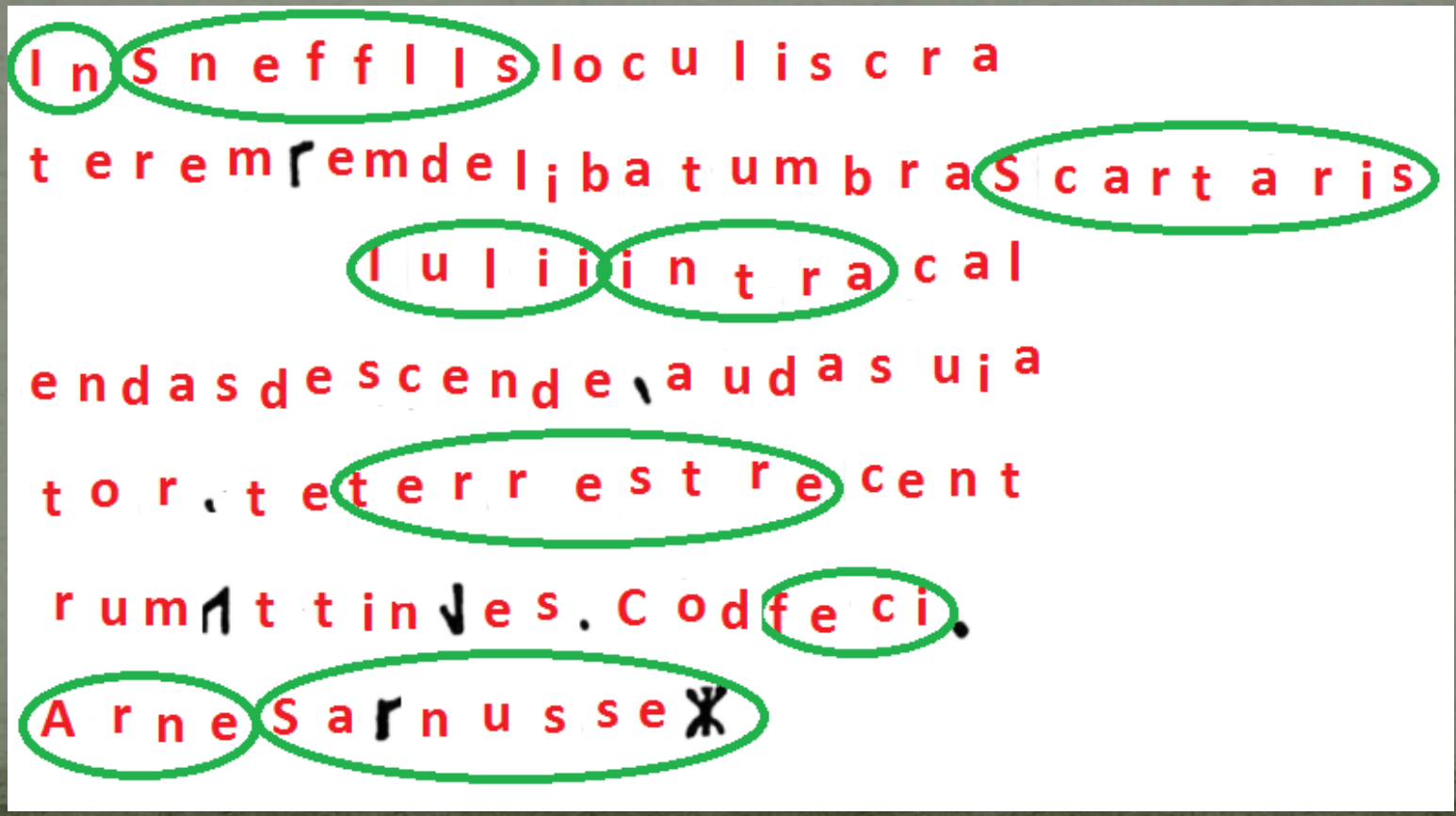
- **Clase de latín (lo siento ☺):**

+Y algunas cosas que vemos son:

-“Ioculus, ioculi": dativo plural "ioculis". Chanza, broma.
-“Cratera, craterae”: forma incorrecta en el texto (sic!) “craterem”. Cráter.
-“Viator, viatoris”: vocativo singular “viator”. Viajero.
-“Calenda, calendae”: acusativo plural “calendas”. Primer día de mes (se refiere al mes de julio, que nombra previamente).
-“Descendo, descendi, descensum”: imperativo presente 2º persona “descende”. Descender.
-“Umbra, umbrae”: nominativo singular, “umbra”. Sombra.
-“Delibo, delibas, delibatum”: presente indicativo 3º persona “delibat”. Acariciar, rozar.
-“Audax, audacis”: forma incorrecta en el texto (sic!) “audas”. Audaz.
-“Centrum, centri”: forma declinada incorrectamente (sic!) “centro”. Centro.

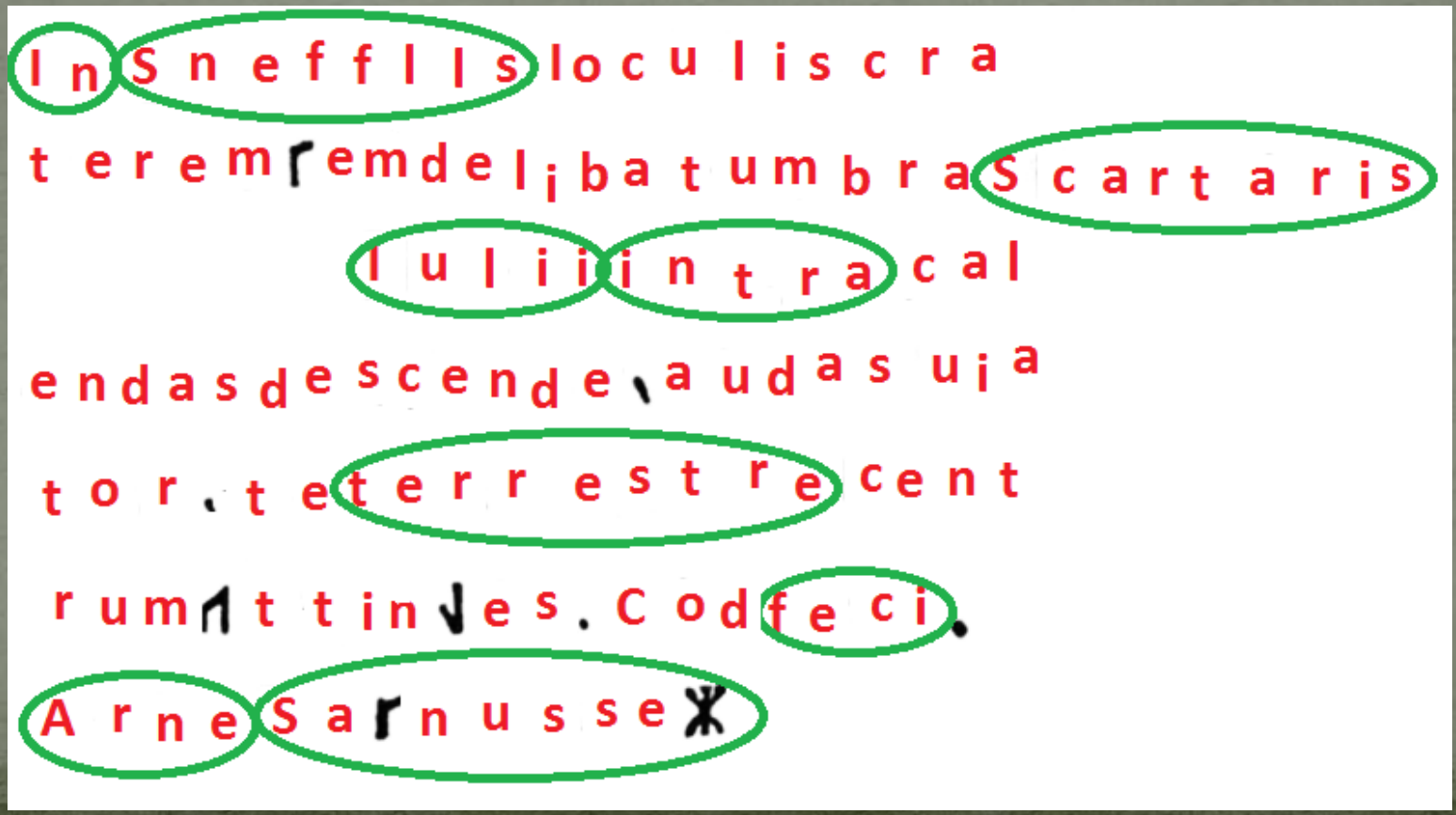
+ Con estas palabras latinas, y a pesar de las incorrecciones lingüísticas, ¡¡que llevan a complicarlo mucho más!!, podemos ofrecer el siguiente texto:





+El texto previo nos indica que expresiones como “cod” se refieren al pronombre relativo “quod”, lo que complica reconocer el texto y el análisis de frecuencias no ayuda.

+Además esto nos lleva a situar como muy probable el signo  , muy cercano al signo “c”,  , como posible sonido “qu”. Y de nuevo otra pista falsa de J. Verne. Porque adopta el valor “k” para el apellido “Saknusse?”.



+¿Y qué decir de los signos pendientes? 

-Lamentablemente, Julio Verne nos vuelve a llevar a error. Ya hemos detectado varios. Indiquemos dos más:

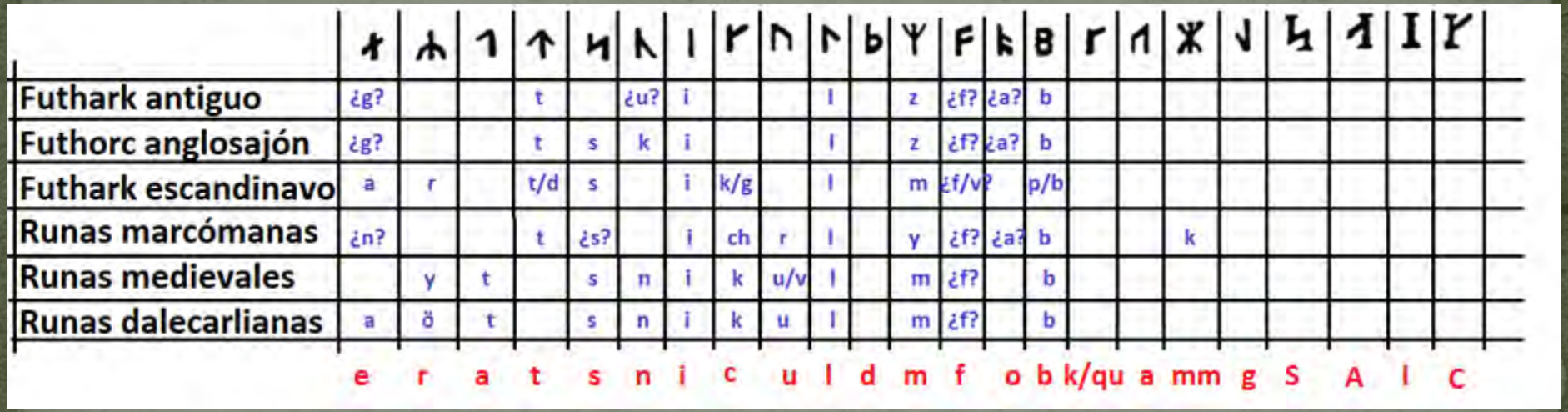
-Error: "te" en lugar de "et".
-Error: "Sneffls" en lugar de "Sneffels".

Ahora vemos que el primero  debería ser  , pues es una "a", y no podía sino ser vocal, pero ya las habíamos agotado todas. Y el verbo es "attingo, atigi, atactum", son significado de "tocar ligeramente". Así, el signo  es una "g".
El restante, es un invento, una "mm",  .

He aquí el texto (con sus errores de varios tipos, para complicas más el criptoanálisis):

"In Sneffls Ioculis craterem quem delibat umbra Scartaris Iulii intra calendas descende, audas uiator, te terrestre centrum attinges. Quod feci.
Arne Saknussemm".

- Volviendo a Julio Verne, y su elección de runas:



Futhark antiguo	¿g?			t		¿u?	i			l		z	¿f?	¿a?	b										
Futhorc anglosajón	¿g?			t	s	k	i			l		z	¿f?	¿a?	b										
Futhark escandinavo	a	r		t/d	s		i	k/g		l		m	¿f/v?		p/b										
Runas marcómanas	¿n?			t	¿s?		i	ch	r	l		y	¿f?	¿a?	b			k							
Runas medievales		y	t		s	n	i	k	u/v	l		m	¿f?		b										
Runas dalecarlianas	a	ö	t		s	n	i	k	u	l		m	¿f?		b										
	e	r	a	t	s	n	i	c	u	l	d	m	f	o	b	k/qu	a	mm	g	S	A	I	C		

+ Y por esto el texto del manuscrito de la edición impresa corrige los errores:

m m.rnlls	esreuel	seecIde
sgtssmf	unteief	niedrke
kt,samn	atrateS	Saodrrn
emtnaeI	nuaect	rrilSa
Atvaar	.nscrc	ieaabs
ccdrmi	eeutul	frantu
dt,iac	oseibo	KediiI

In Sneffels Ioculis craterem kem delibat umbra Scartaris Iulii intra calendas descende, audas viator, et terrestre centrum attinges. Kod feci. Arne Saknussemm.

NOTA: "Jökull" en islandés significa glaciar.
Suele formar parte del nombre de muchos picos de las islas.
Julio Verne en la novela lo traduce como "ventisquero". (No es latín).

"Desciende el cráter del Sneffelsjökull,
que la sombra del Scartaris acaricia antes del mes de julio,
y llegarás al centro de la tierra, como he hecho yo.
Arne Saknussemm".

CRIPTOANÁLISIS

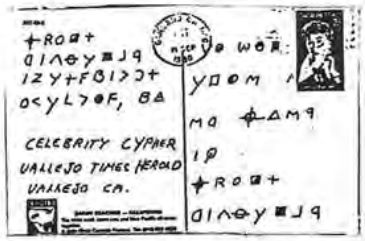
-Rompiendo algoritmos criptográficos

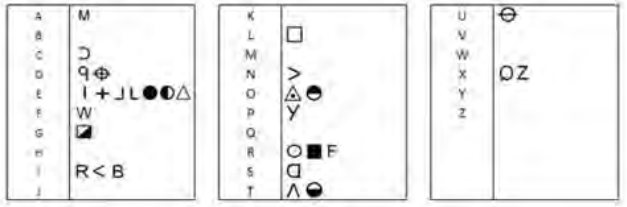
Empecemos por la (a).....que puede ser a veces muy complicada.

CIFRADO DE SUSTITUCIÓN

I-Asesino del Zodiaco (5 asesinatos a finales de los años 60 del siglo XX. Varias cartas y entre ellas varios criptogramas).

II-Mensaje descifrado





CRIPTOANÁLISIS

-Rompiendo algoritmos criptográficos

Empecemos por la (a)..... que puede ser a veces muy complicada.

KRYPTOS (C.I.A.)

Escultura criptográfica en la sede de Langley (Virg).

Cuatro enigmas resueltos desde su creación (3-Nov-1990). Queda uno pendiente.

TENEMOS QUE EXPLICAR ALGUNAS COSAS PREVIAS PARA VER LOS ATAQUES DE CANAL LATERAL

-Las clases de cifrado (modernamente entendido):

§ Simétrica (clave privada)

§ Asimétrica (clave pública)

TENEMOS QUE EXPLICAR ALGUNAS COSAS PREVIAS PARA VER LOS ATAQUES DE CANAL LATERAL

-Las clases de cifrado (modernamente entendido):

§ Simétrica (clave privada)

+ Cifrado

+ Rapidez frente a la asimétrica

§ Asimétrica (clave pública)

+ Cifrado

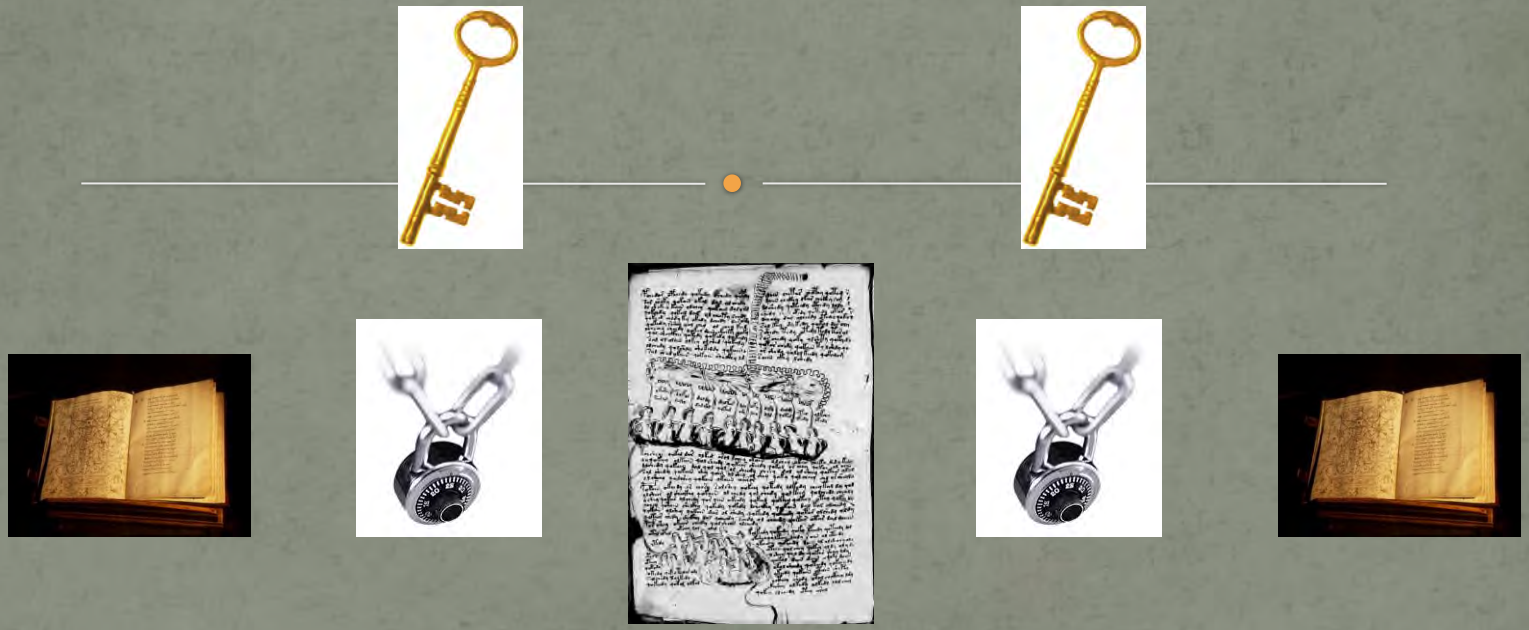
+ Autenticación

+ No repudio

+ Intercambio de claves

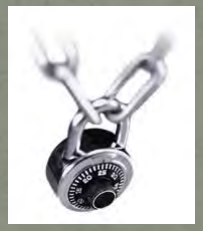
TENEMOS QUE EXPLICAR ALGUNAS COSAS PREVIAS PARA VER LOS ATAQUES DE CANAL LATERAL

-Cifrado simétrico

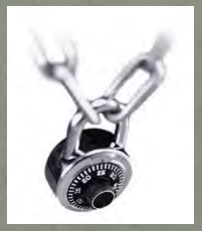


TENEMOS QUE EXPLICAR ALGUNAS COSAS PREVIAS PARA VER LOS ATAQUES DE CANAL LATERAL

-Cifrado asimétrico



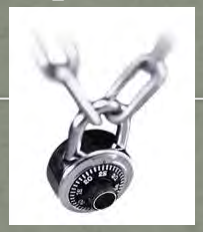


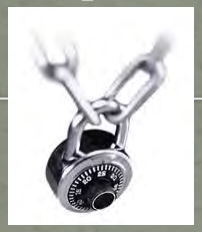

TENEMOS QUE EXPLICAR ALGUNAS COSAS PREVIAS PARA VER LOS ATAQUES DE CANAL LATERAL

-Cifrado asimétrico

Clave privada A

Clave privada B





Claves públicas de A, B, C,…

LOS CIFRADOS QUE VAMOS A CRACKEAR

Cifrador DES

-Data Encryption Standard (DES) o Data Encryption Algorithm (DEA):

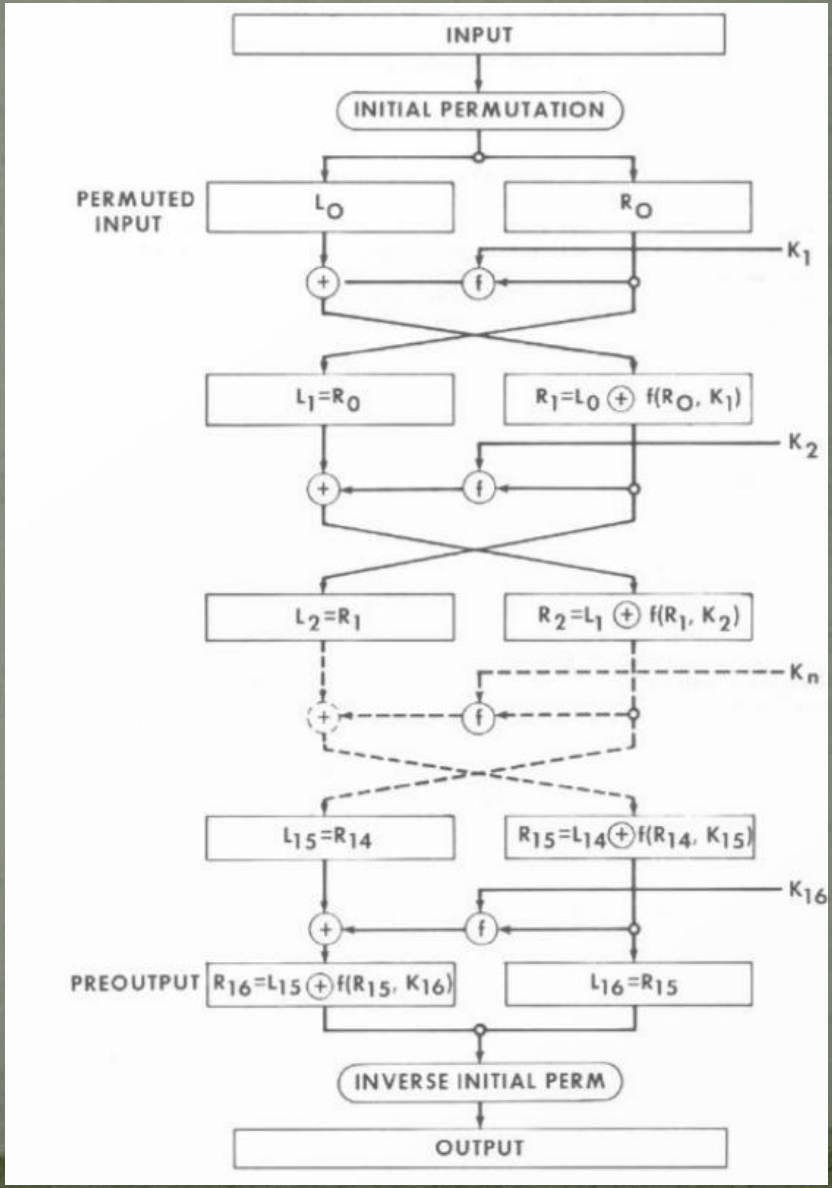
-Estándar (1976).
-Proviene de Lucifer de Horst Feistel en la IBM.
-Reemplazado en el año 2.002 por el cifrado AES (Advanced Encryption Standard).
-Sigue usándose (T-DES).
-El más estudiado y analizado.

-Cifrado en bloque de 64 bits y salida similar.
-Clave criptográfica de 64 bits con 8 de paridad.
-Ataque por fuerza bruta: 2^{56}.
-DES Cracker: Electronic Frontier Foundation (EFF), 250.000 $, 1.856 chips, 56 horas (1998).

LOS CIFRADOS QUE VAMOS A CRACKEAR

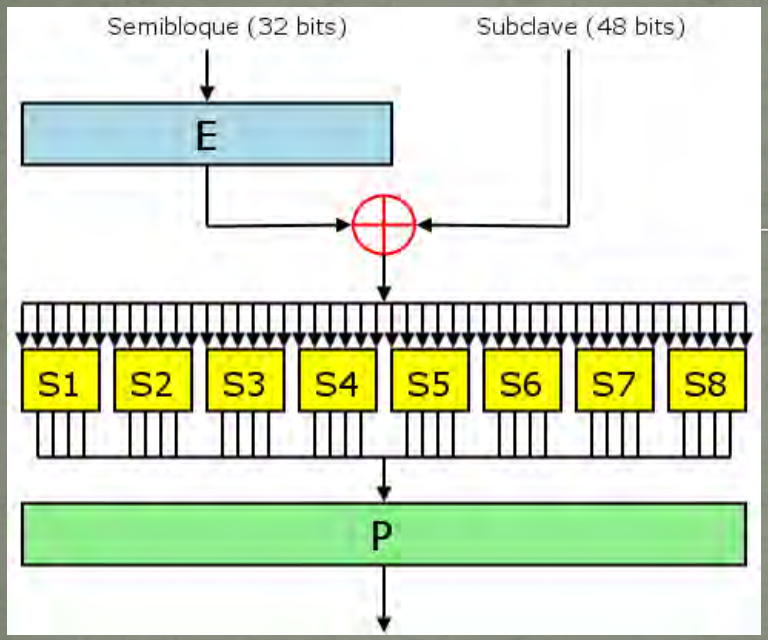
Cifrador DES

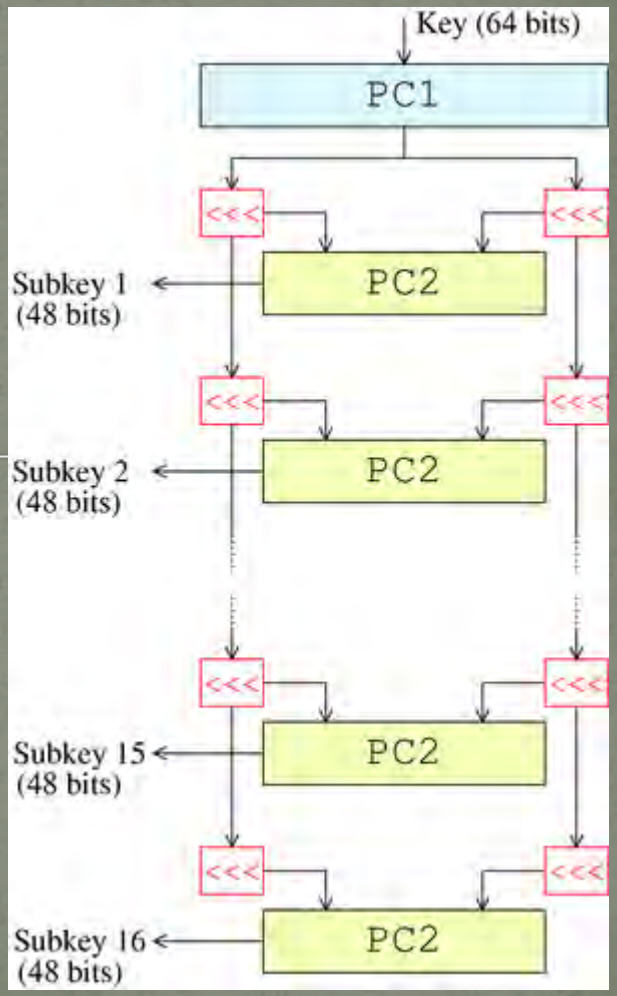
-Esquema general



LOS CIFRADOS QUE VAMOS A CRACKEAR

Cifrador DES





-Función f (Feistel).
-Generador de subclaves.

LOS CIFRADOS QUE VAMOS A CRACKEAR

Cifrador DES

PC-1: Permuted Choice 1

Bit	0	1	2	3	4	5	6
1	57	49	41	33	25	17	9
8	1	58	50	42	34	26	18
15	10	2	59	51	43	35	27
22	19	11	3	60	52	44	36
29	63	55	47	39	31	23	15
36	7	62	54	46	38	30	22
43	14	6	61	53	45	37	29
50	21	13	5	28	20	12	4

PC-2: Permuted Choice 2

Bit	0	1	2	3	4	5
1	14	17	11	24	1	5
7	3	28	15	6	21	10
13	23	19	12	4	26	8
19	16	7	27	20	13	2
25	41	52	31	37	47	55
31	30	40	51	45	33	48
37	44	49	39	56	34	53
43	46	42	50	36	29	32

-Permutaciones 1 y 2.

-Rotaciones de las subclaves.

Subkey Rotation Table

Round Number	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Number of bits to rotate	1	1	2	2	2	2	2	2	1	2	2	2	2	2	2	1

LOS CIFRADOS QUE VAMOS A CRACKEAR

Cifrador DES

IP: Initial Permutation

Bit	0	1	2	3	4	5	6	7
1	58	50	42	34	26	18	10	2
9	60	52	44	36	28	20	12	4
17	62	54	46	38	30	22	14	6
25	64	56	48	40	32	24	16	8
33	57	49	41	33	25	17	9	1
41	59	51	43	35	27	19	11	3
49	61	53	45	37	29	21	13	5
57	63	55	47	39	31	23	15	7

IP^(-1): Inverse Initial Permutation

Bit	0	1	2	3	4	5	6	7
1	40	8	48	16	56	24	64	32
9	39	7	47	15	55	23	63	31
17	38	6	46	14	54	22	62	30
25	37	5	45	13	53	21	61	29
33	36	4	44	12	52	20	60	28
41	35	3	43	11	51	19	59	27
49	34	2	42	10	50	18	58	26
57	33	1	41	9	49	17	57	25

-Permutaciones inicial y final.

LOS CIFRADOS QUE VAMOS A CRACKEAR

Cifrador DES

E-Bit Selection Table

Bit	0	1	2	3	4	5
1	32	1	2	3	4	5
7	4	5	6	7	8	9
13	8	9	10	11	12	13
19	12	13	14	15	16	17
25	16	17	18	19	20	21
31	20	21	22	23	24	25
37	24	25	26	27	28	29
43	28	29	30	31	32	1

P Permutation

Bit	0	1	2	3
1	16	7	20	21
5	29	12	28	17
9	1	15	23	26
13	5	18	31	10
17	2	8	24	14
21	32	27	3	9
25	19	13	30	6
29	22	11	4	25

-Selección del bit E, y permutación P.

LOS CIFRADOS QUE VAMOS A CRACKEAR

Cifrador DES

S-Box 1: Substitution Box 1

Row / Column	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
1	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
2	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
3	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

S-Box 2: Substitution Box 2

Row / Column	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10
1	3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5
2	0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15
3	13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9

S-Box 3: Substitution Box 3

Row / Column	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8
1	13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1
2	13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7
3	1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12

S-Box 4: Substitution Box 4

Row / Column	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15
1	13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9
2	10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4
3	3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14

-S-boxes 1, 2, 3, 4.

LOS CIFRADOS QUE VAMOS A CRACKEAR

Cifrador DES

S-Box 5: Substitution Box 5

Row / Column	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9
1	14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6
2	4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14
3	11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3

S-Box 6: Substitution Box 6

Row / Column	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	12	1	10	15	9	2	6	8	0	13	3	4	14	7	5	11
1	10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8
2	9	14	15	5	2	8	12	3	7	0	4	10	1	13	11	6
3	4	3	2	12	9	5	15	10	11	14	1	7	6	0	8	13

S-Box 7: Substitution Box 7

Row / Column	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	4	11	2	14	15	0	8	13	3	12	9	7	5	10	6	1
1	13	0	11	7	4	9	1	10	14	3	5	12	2	15	8	6
2	1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	2
3	6	11	13	8	1	4	10	7	9	5	0	15	14	2	3	12

S-Box 8: Substitution Box 8

Row / Column	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7
1	1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2
2	7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8
3	2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11

-S-boxes 5, 6, 7, 8.

LOS CIFRADOS QUE VAMOS A CRACKEAR

Cifrador DES: Criptoanálisis lineal (Mitsuru Matsui)

+Confusión y difusión en los criptosistemas.

+Elementos lineales y no lineales.

(a) Permutaciones: Lineales.

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 4 & 5 & 7 & 6 & 1 & 8 & 2 \end{pmatrix}$$

(b) Sustituciones (S-box): No lineales.

$$\xi = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & A & B & C & D & E & F \\ 8 & F & 1 & C & 6 & 3 & 9 & 0 & 2 & A & E & 5 & 4 & B & 7 & D \end{pmatrix}$$

(c) Mezcla de sub-claves: Lineales.

$K_i / i \in \{1, ..., n\}$

XOR

LOS CIFRADOS QUE VAMOS A CRACKEAR

Cifrador DES: Criptoanálisis lineal (Mitsuru Matsui)

+Lema Piling Up

$$\begin{cases} X_1 \oplus X_2 = 0 \\ X_1 = X_2 \end{cases}$$

$$\begin{cases} X_1 \oplus X_2 = 1 \\ X_1 \neq X_2 \end{cases}$$

$$Pr(X_1 = i) \begin{cases} p_1 & i = 0 \\ 1 - p_1 & i = 1 \end{cases}$$

$$Pr(X_2 = i) \begin{cases} p_2 & i = 0 \\ 1 - p_2 & i = 1 \end{cases}$$

+Suponemos independencia de variables:

$$Pr(X_1 = i, X_2 = j) \begin{cases} p_1 p_2 & i = 0, j = 0 \\ p_1(1 - p_2) & i = 0, j = 1 \\ (1 - p_1)p_2 & i = 1, j = 0 \\ (1 - p_1)(1 - p_2) & i = 1, j = 1 \end{cases}$$

$$Pr(X_1 \oplus X_2 = 0) = Pr(X_1 = X_2) = Pr(X_1 = 0, X_2 = 0) + Pr(X_1 = 1, X_2 = 1) = p_1 p_2 + (1 - p_1)(1 - p_2)$$

$$p_1 = 1/2 + \varepsilon_1$$

$$p_2 = 1/2 + \varepsilon_2$$

$$\varepsilon_1, \varepsilon_2 \in [-1/2, 1/2]$$

$$Pr(X_1 \oplus X_2 = 0) = 1/2 + 2\varepsilon_1\varepsilon_2$$

LOS CIFRADOS QUE VAMOS A CRACKEAR

Cifrador DES: Criptoanálisis lineal (Mitsuru Matsui)

+Lema Piling Up

$$X_1 \oplus ... \oplus X_n = 0$$

+Generalizando:

$$Pr(X_1 \oplus ... \oplus X_n = 0) = 1/2 + 2^{n-1} \prod_{i=1}^{n} \varepsilon_i$$

$$\varepsilon_{1,2,...,n} = 2^{n-1} \prod_{i=1}^{n} \varepsilon_i$$

-Criptoanálisis Lineal: M. Matsui (1993). 2^{43} textos planos escogidos, y 2^{41} al paralelizarse (Kaliski, Robshaw, Biryukov).
Desconocido por la IBM al desarrollar DES.

OTROS ATAQUES CRIPTOANALÍTICOS AL CIFRADO DES

-Criptoanálisis Diferencial: E.Biham, A. Shamir (´80). 2^{47} textos planos escogidos. Conocido por la IBM al desarrollar DES.

-Criptoanálisis Davies o Imposible: D. Davies (´80), y mejoras de Biham, Shamir y Biryukov. 2^{50} textos planos escogidos.

-Criptoanálisis Lineal-Diferencial: Langford y Hellman (1.994). 9/16 rondas con 2^{16} textos planos conocidos.

OTROS CIFRADORES SIMÉTRICOS

-T-DES, X-DES, AES (Rijndael), 3-Way, ABC, Anubis, BATON, Blowfish, Camellia, CAST-128, CAST-256, CMEA, CRYPTON, CIPHERUNICORN, DEAL, DFC, E2, FEAL, FROG, GOST, Hierocrypt, HPC, IDEA, KHAZAD, LOKI89, MAGENTA, MARS, MISTY1, RC2, RC5, RC6, SC2000, SAFER, SERPENT, SHACAL, Skipjack, TEA, Threefish, Twofish…

EE.UU (2002): AES

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

NESSIE
New European Schemes for Signatures, Integrity, and Encryption

Europa (2000-2003): MISTY1, Camellia, SHACAL-2, AES

CRYPTREC
Cryptography Research and Evaluation Committees

Japón (2000-2003): AES, Camellia, CIPHERUNICORN-A, CIPHERUNICORN-E, Hierocrypt-L1, Hierocrypt-3, MISTY1, SC2000, T-DES

OTROS CIFRADORES SIMÉTRICOS (de flujo, no de bloque)

-A5/1, A5/2, A5/3, BMGL, Chamaleon, Dragon, FISH, Grain, HC-128, HC-256, ISAAC, Leviathan, LILI-128, MICKEY, MUGI, MULTI-S01, Panama, Phelix, Pike, Py, Rabbit, RC4, RCR32/64, Salsa20, Scream, SEAL, SNOW, SOBER, SOSEMANUK, TPy, TPypy, TPy6, Trivium, Turing, VEST...

Europa (2004-2008):
Software: HC-128, Rabbit, Salsa20/12, SOSEMANUK.

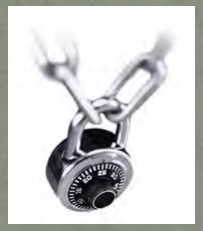
Hardware: Grain, MICKEY, Trivium.

CRYPTREC
Cryptography Research and Evaluation Committees

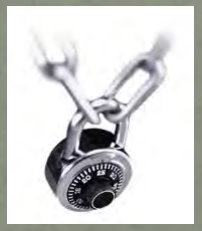
Japón (2000-2003): MUGI, MULTI-S01, RC4

TENEMOS QUE EXPLICAR ALGUNAS COSAS PREVIAS PARA VER LOS ATAQUES DE CANAL LATERAL

-Cifrado asimétrico

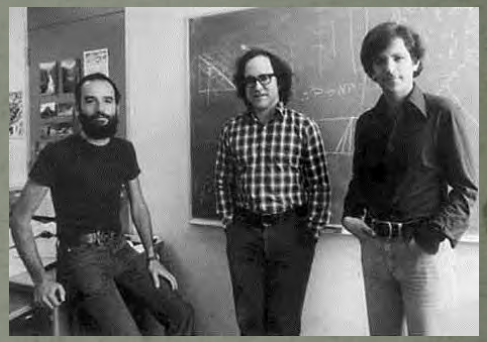








LOS CIFRADOS QUE VAMOS A CRACKEAR

Cifrador RSA



RSA (Rivest, Shamir, Adleman): 1977

INTEGER FACTORIZATION PROBLEM (IFP):

Dado $r=pq \;/\; p,q \text{ primos}$

determinar los factores de *r: p, q.*

LOS CIFRADOS QUE VAMOS A CRACKEAR

Cifrador RSA

Elementos estructurales necesarios al Algoritmo RSA:
Dos números primos p y q.
$r = pq$
$\phi(r) = (p-1)(q-1)$
SK (Secret Key) es la Clave Privada
PK (Public Key) es la Clave Pública
X es el mensaje a transmitir o texto plano
Y es el mensaje recibido ya cifrado

$$SK \times PK \equiv 1 \bmod \phi(r)$$

$$X^{SK \times PK} \equiv X \bmod r$$

Esquema de cifrado:

Cifrado:

$$E_{PK}(X) = Y \equiv X^{PK} \bmod r .$$

Descifrado:

$$D_{SK}(Y) \equiv Y^{SK} \bmod r \equiv X^{PK \times SK} \bmod r \equiv X \bmod r .$$

LOS CIFRADOS QUE VAMOS A CRACKEAR

Cifrador RSA

p=47	Elegido
q=61	Elegido
R=pq=47*61=2867	Derivado
$\phi(r)$=(p-1)*(q-1)=46*60=2760	Derivado
SK=167	Elegido
PK=1223	Derivado

A=00, B=01,…Z=25

mensaje "ALGORITMORSA".

"AL GO RI TM OR SA"

[0011, 0614, 1708, 1912, 1417, 1800]

Esquema de cifrado:

Cifrado:

$$E_{PK}(X) = Y \equiv X^{PK} \bmod r .$$

[2185, 0222, 0488, 1557, 1085, 0299]

Descifrado:

$$D_{SK}(Y) \equiv Y^{SK} \bmod r \equiv X^{PK \times SK} \bmod r \equiv X \bmod r .$$

[0011, 0614, 1708, 1912, 1417, 1800]

LOS CIFRADOS QUE VAMOS A CRACKEAR

Cifrador RSA

ATAQUES AL IFP. RSA-200:

• 200 dígitos decimales. 663 bits

27997833911221327870829467638722601621070446786955428537560009929326128400107609345671052955360856061822351910951365788637105954482006576775098580557613579098734950144178863178946295187237869221823983

• 9-Mayo-2005. Bahr, Boehm, Franke, Kleinjung. NFS

35324619344027701212726049781984643686711974001976250236493034687761212536794232000585479565280883497925869954478333033347085841480059687737975857364219960734330341455767872818 152135381409304740185467

OTROS CIFRADORES ASIMÉTRICOS

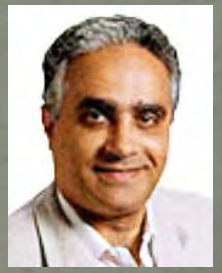
ElGamal

(Diffie, Hellman, Merkle; 1976. ElGamal; 1984)

DISCRETE LOGARITHM PROBLEM (DLP):

Dado $y, p, g \;/\; y = g^x \bmod p$

determinar *x*.



OTROS CIFRADORES ASIMÉTRICOS

Curva Elíptica

(Miller, Koblitz; 1985)

ELLIPTIC CURVE - DISCRETE LOGARITHM PROBLEM

(EC-DLP):

Dado `E(K) y Q y P puntos / Q=m*P`

determinar *m*.

OTROS CIFRADORES ASIMÉTRICOS

- Mochila con Trampa (Chor-Rivest, etc.), McEliece, Benaloh, Blum-Goldwasser, Cayley-Purser, CEILIDH, Cramer-Shoup, Damgård-Jurik, Goldwasser-Micali, HFE, Naccache-Stern, NTRUEncrypt, Paillier, Rabin, Okamoto-Uchiyama, XTR.

EE.UU (2002): RSA, Curva Elíptica

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

NESSIE
New European Schemes for Signatures, Integrity, and Encryption

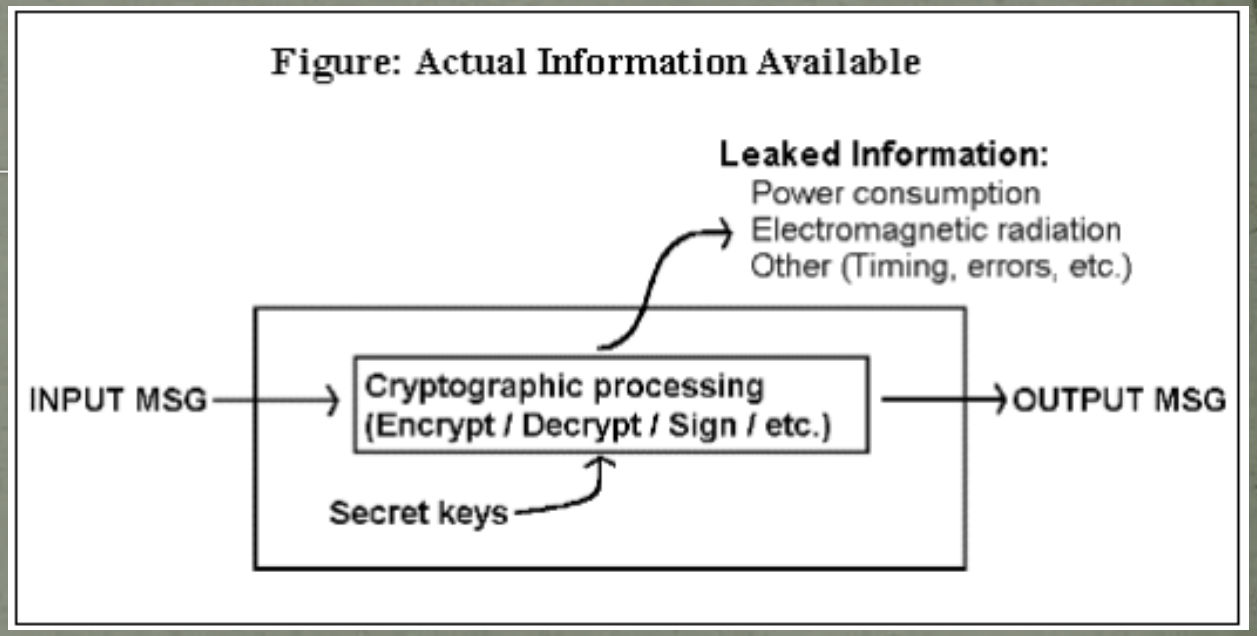
Europa (2000-2003): RSA, Curva Elíptica

CRYPTREC
Cryptography Research and Evaluation Committees

Japón (2000-2003): RSA, Curva Elíptica

ATAQUES DE CANAL LATERAL

Seguimos por la (b)…..



ENTRE INVASIONES Y ABORDAJES

-Ataques no invasivos: los más baratos (menos caros).

+Observan y manipulan el dispositivo sin daño físico.
+Equipo semisofisticado y conocimientos semielevados.

+Equipo: Multímetro digital, estación de desoldado, osciloscopio, generador de señales, analizador lógico, banco de testeo de circuitos integrados, placa FPGA, PC y periférico de adquisición de datos,…

-Ataque invasivos: los más caros.

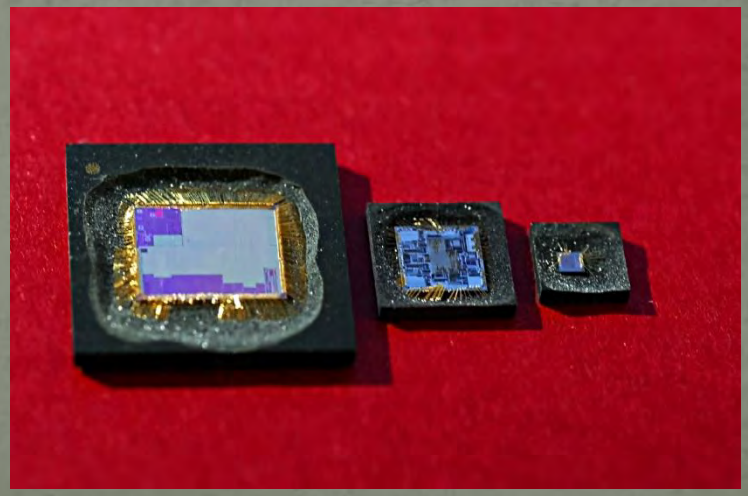
+Dejan evidencia de la manipulación ("tamper-evidence"), y muchas veces dejan inservible el dispositivo.
+Máximo de capacidades técnicas y elevados conocimientos hardware.
A veces, mucho tiempo.
+Equipo: Añadimos a los anteriores un laboratorio químico, microscopio óptico de alta resolución, cortadora láser, estación de micro sondeo, microscopio de electrones, estación de iones focalizados.

ENTRE INVASIONES Y ABORDAJES

Desencapsulado

-Gases de ácido nítrico (HNO_3) a 60ºC y baño de acetona.
-Mezcla de ácido nítrico (HNO_3) y sulfúrico (H_2SO_4).

-Total o parcial.



ENTRE INVASIONES Y ABORDAJES

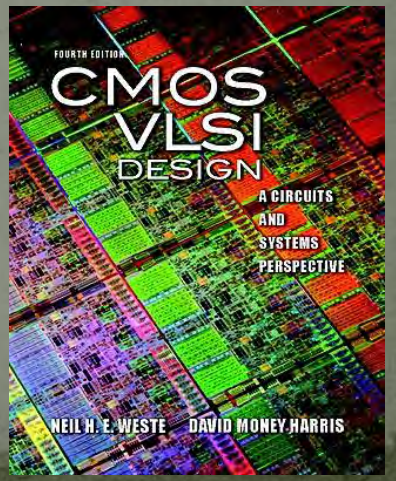
Reconstrucción del "layout":

-Construir el mapa: estructura arquitectural, líneas de datos, de direcciones, conectividades, metalizaciones, fronteras,…

-Subcapas: eliminación tras baño de ácido fluorhídrico de las capas que las recubren, quitando el óxido de silicio.

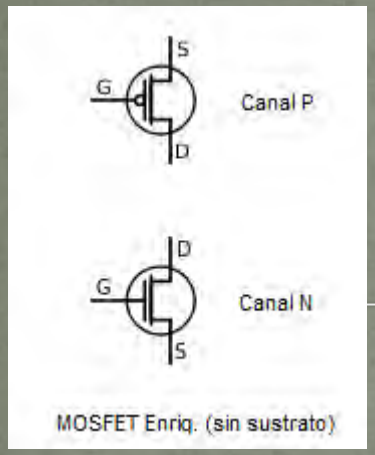
-Conocimientos en tecnología CMOS VLSI y microscopía.

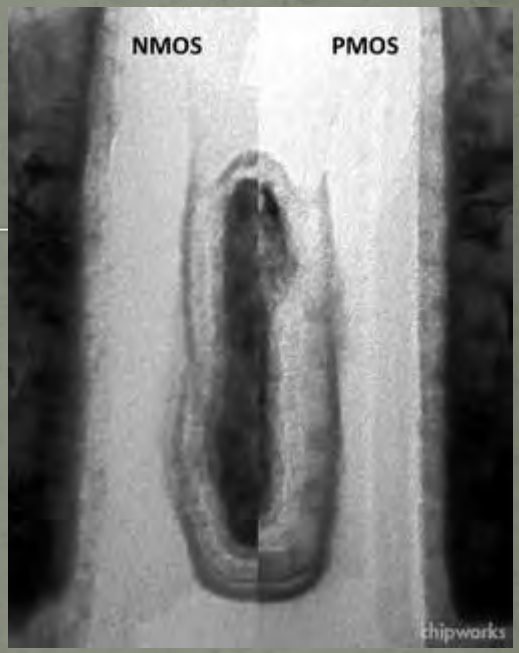
-¿Arquitectura estándar, bloques conocidos, módulos funcionales, hardware propietario…? Dependerá…

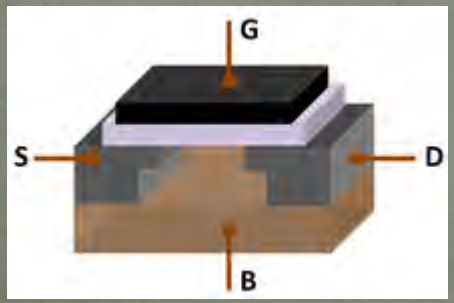


ENTRE INVASIONES Y ABORDAJES

Reconstrucción del "layout":

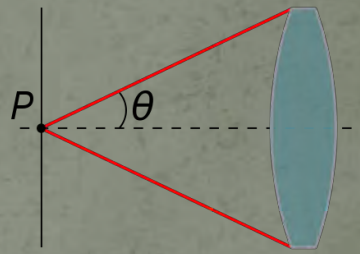






ENTRE INVASIONES Y ABORDAJES

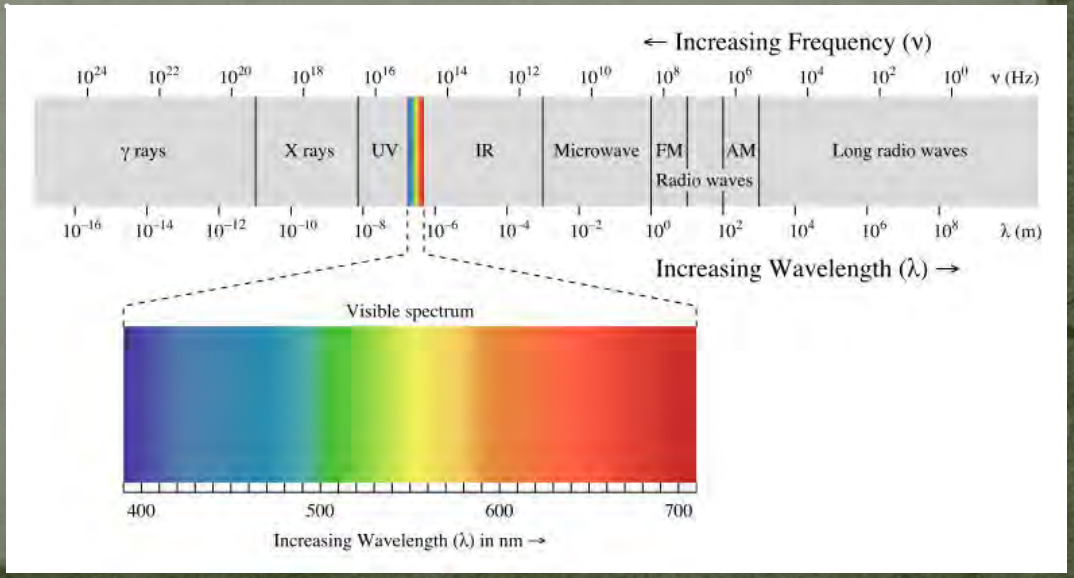
Reconstrucción del "layout": Imagen óptica.



-Se puede llegar a los 0.18µm (y en UV sin ataque químico).

-NA=n×sinθ
-Resolución R=0,61λ/NA

+Subir índice de refracción del medio (inmersión en aceite: n=1,5).
+Aumentar el valor de la Apertura Numérica NA .
+Reducir longitud de onda (en UV).

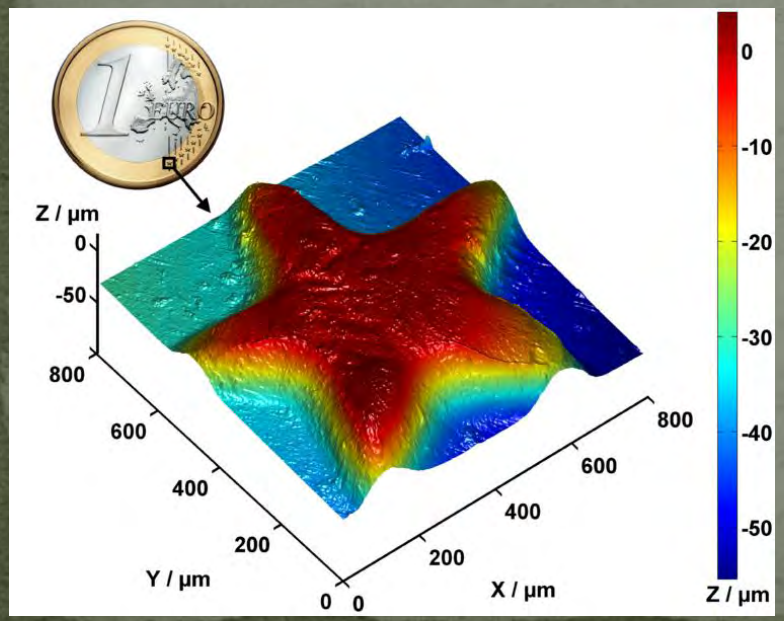


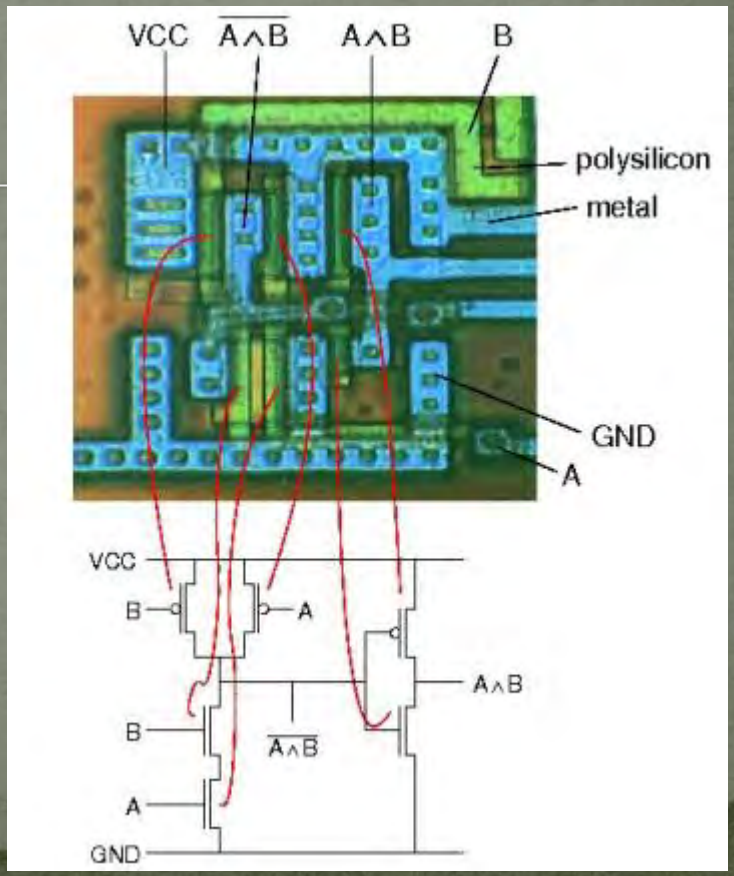
ENTRE INVASIONES Y ABORDAJES

Reconstrucción del "layout": Imagen con microscopio confocal.

-La lectura de las operaciones de los CMOS en el circuito integrado pueden hacerse con facilidad (tras experiencia), permitiendo el microscopio confocal representar los "layers" en distintos colores.

-El microscopio confocal (0,5µm) permite así por medio de los contrastes realizar imágenes tridimensionales.





ENTRE INVASIONES Y ABORDAJES

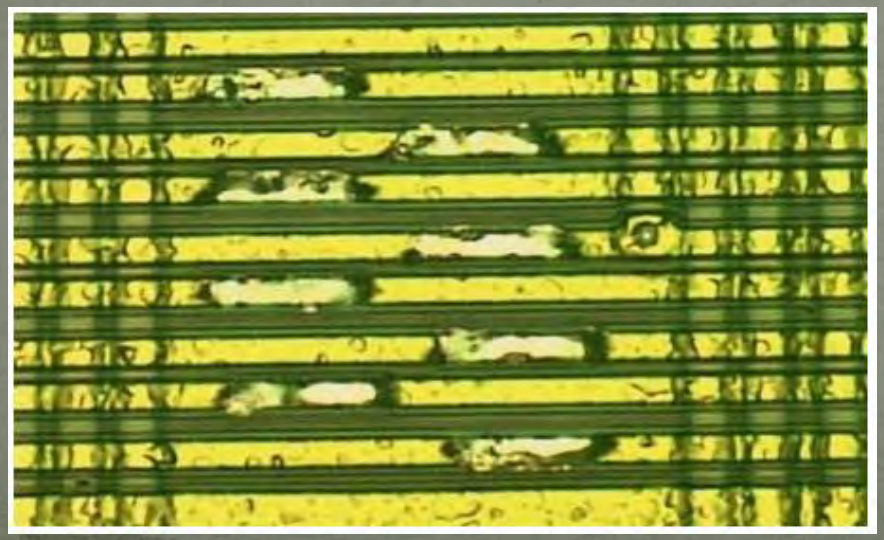
Reconstrucción del "layout": Imagen con microscopio electrónico.

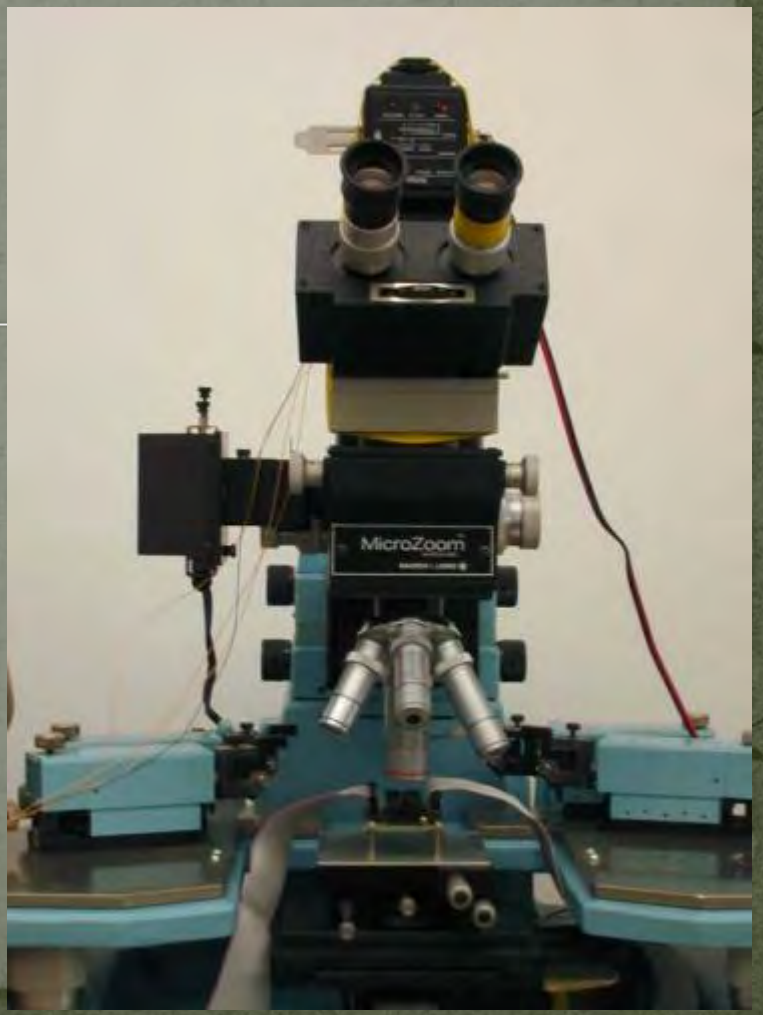
-La longitud de onda de los electrones (λ_e) es 100.000 menor que la de los fotones (λ_γ).

ENTRE INVASIONES Y ABORDAJES

Microsondas (microprobing)

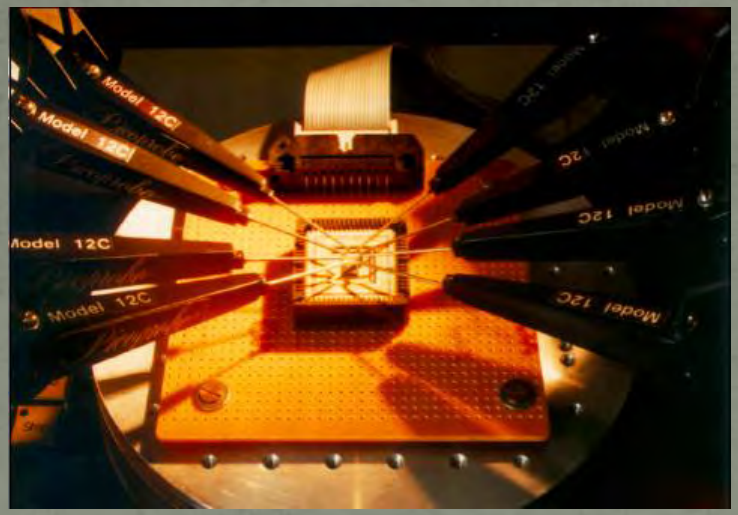
-Observación de señales en el chip.
-Inyección de señales test y observación de salidas.
-Límite en los 0,30µm.
-Cortes laser
(eliminar la capa pasiva para los contactos).
-Coste material: miles de €.





ENTRE INVASIONES Y ABORDAJES

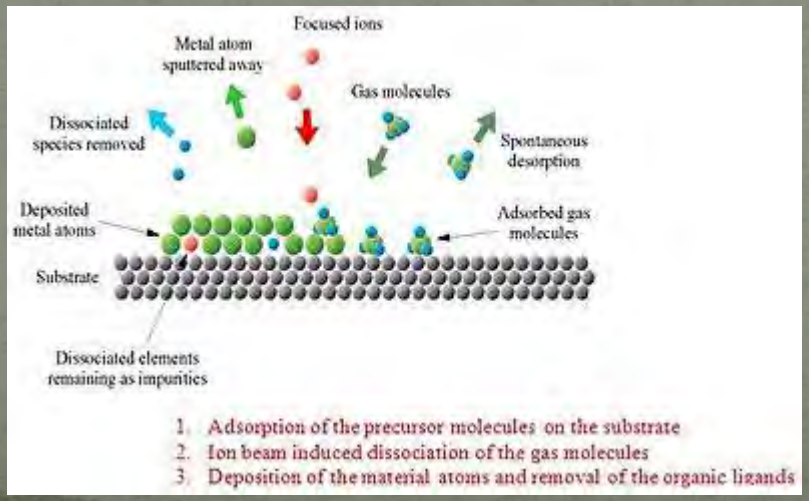
Microsondas (microprobing)

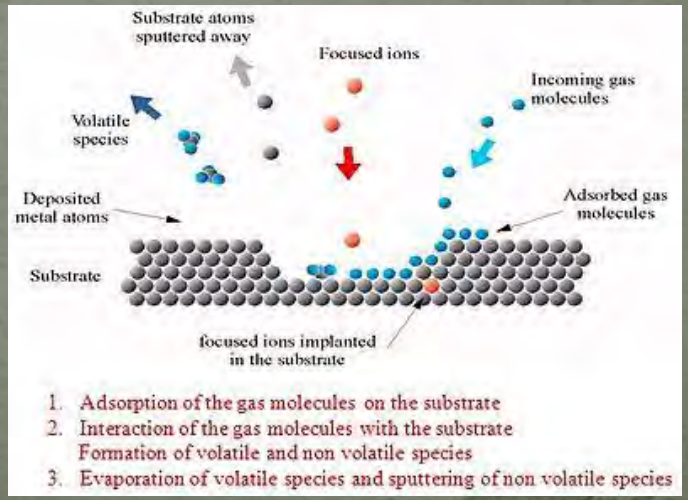


ENTRE INVASIONES Y ABORDAJES

Estación de rayo de iones focalizados (FIB)

-Microcirugía a 5-10nm.
-Iones de Galio acelerados.
-Arranca material perforando a baja profundidad y ángulos diversos, y deposita material (platino).
-Modificación del circuito integrado: cierra conexiones, crea nuevas,…
-Ayuda al microprobing con la deposición platínica, y ataca al chip por detrás.
-Coste material: miles de €.

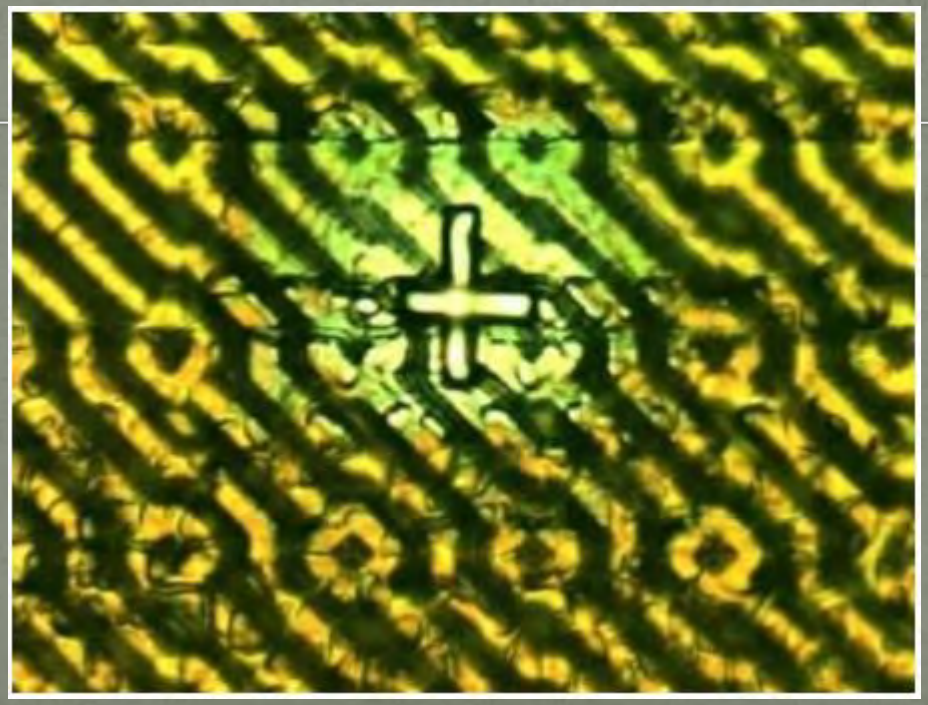




ENTRE INVASIONES Y ABORDAJES

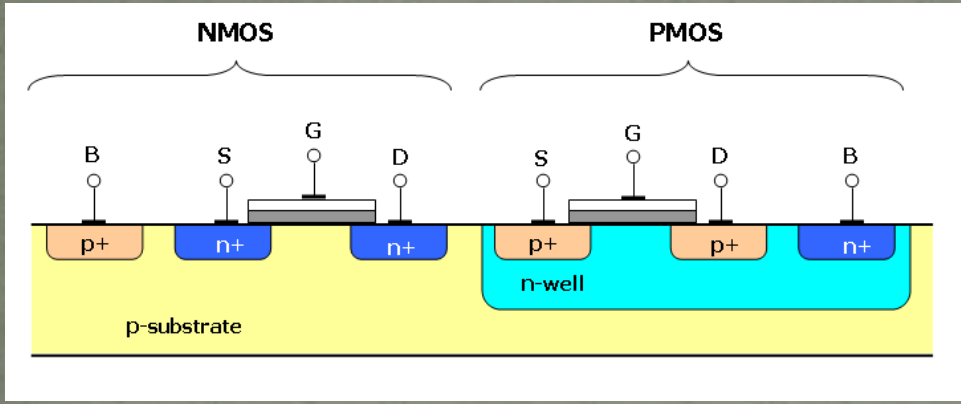
Estación de rayo de iones focalizados (FIB)

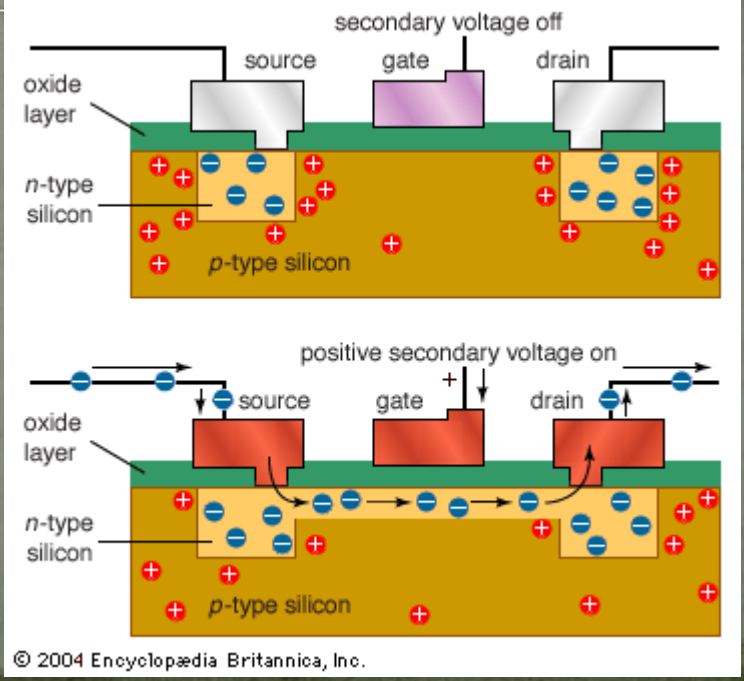
-Ayuda al microprobing con la deposición platínica.



ANÁLISIS DE POTENCIA (SPA y DPA)

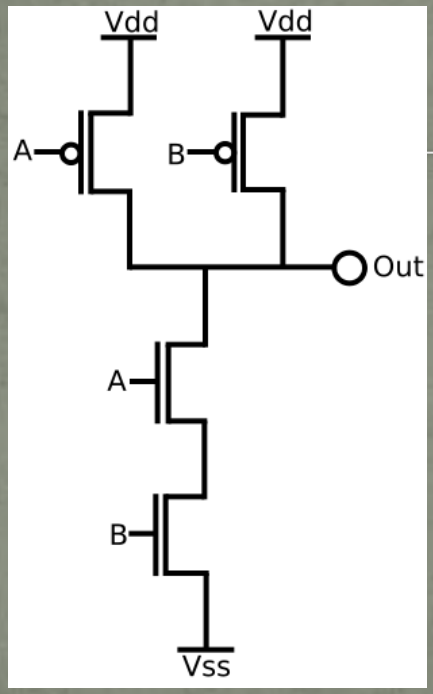
-Estructura CMOS

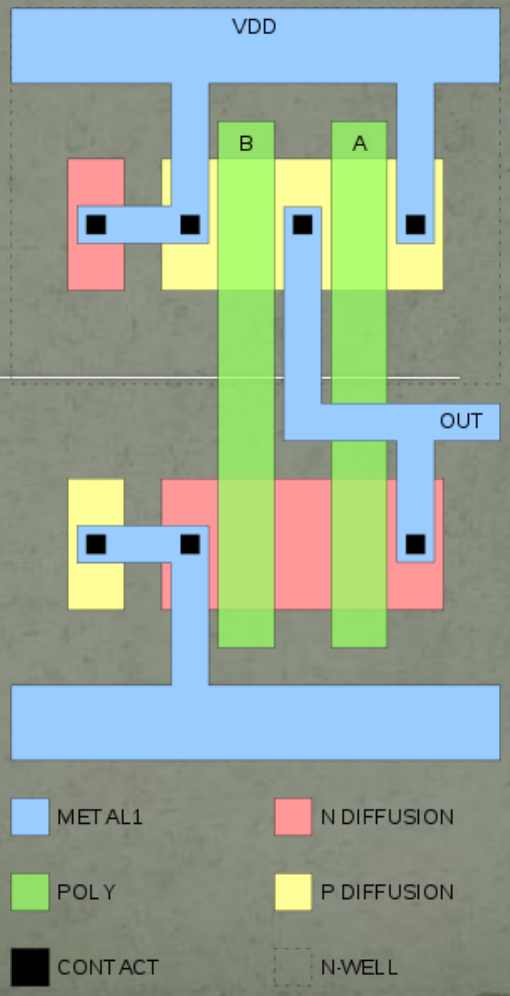




ANÁLISIS DE POTENCIA (SPA y DPA)

-Estructura CMOS: Puerta NAND





ANÁLISIS DE POTENCIA (SPA y DPA)

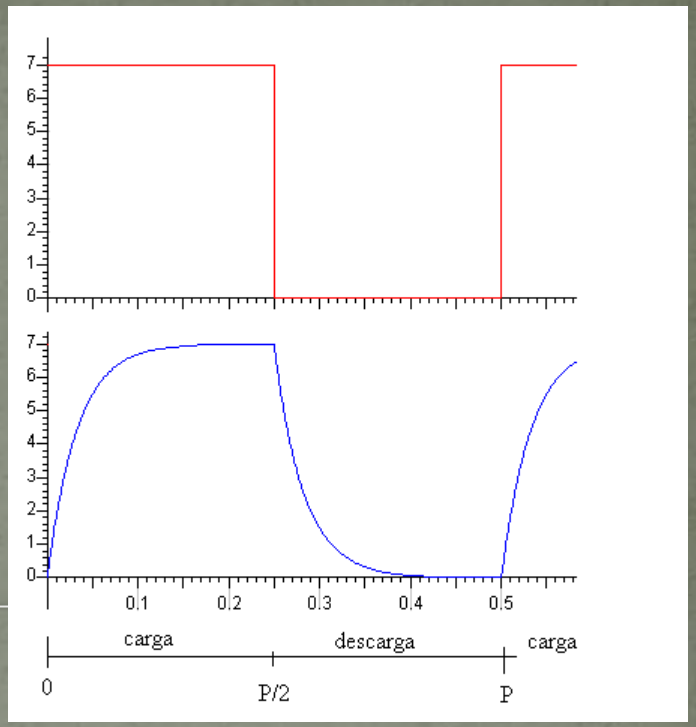
-Disipación de potencia:

Tipos de disipación:

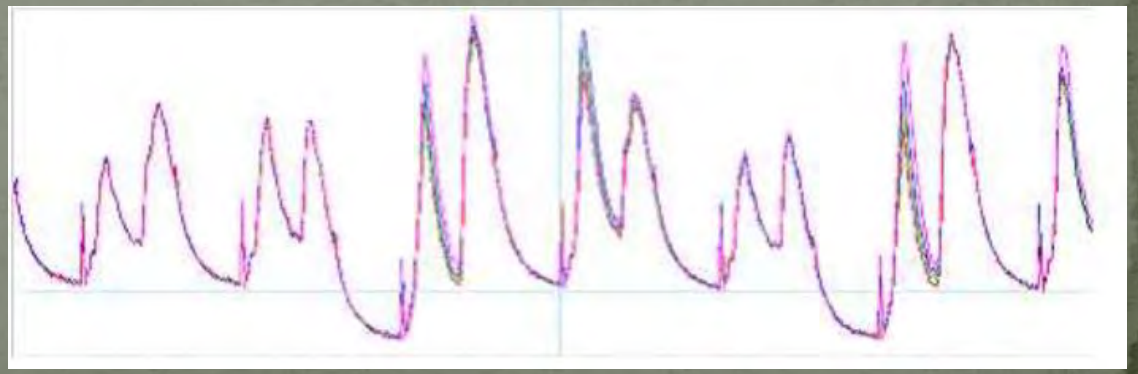
+(a)Disipación estática

+(b) Disipación dinámica:

-(b) Es la que nos interesa aquí.
-Carga y descarga de las capacidades.

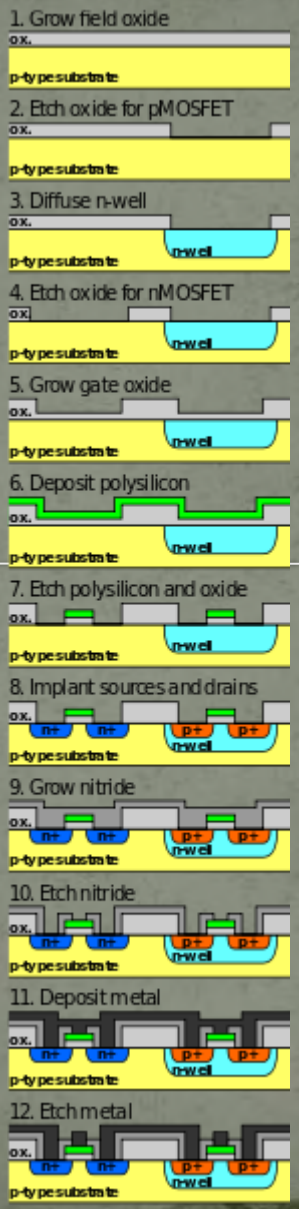


$$P=CV^2f$$



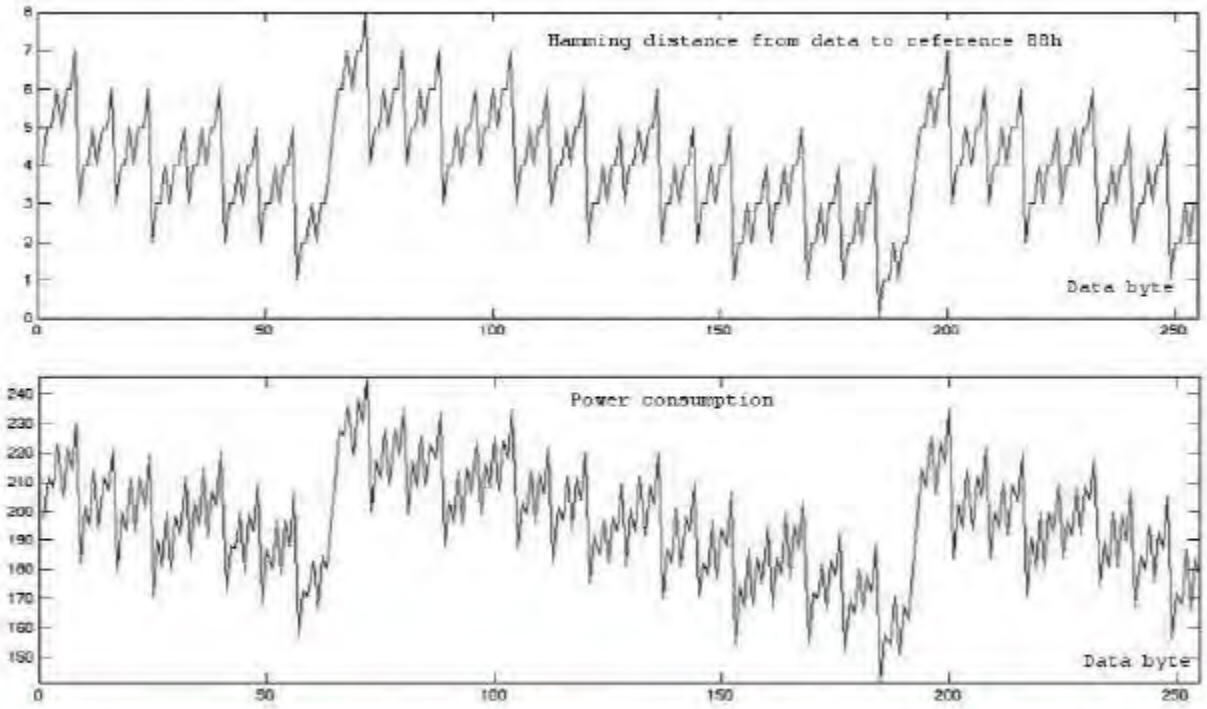
ANÁLISIS DE POTENCIA (SPA y DPA)

-Estructura CMOS: fabricación



ANÁLISIS DE POTENCIA (SPA y DPA)

8º	7º	6º	5º	4º	3º	2º	1º	Distancia Hamming
0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	1	1
0	0	0	0	0	0	1	0	1
0	0	0	0	0	0	1	1	2
0	0	0	0	0	1	0	0	1
0	0	0	0	0	1	0	1	2
...	...	...	...	...	...	...	...	...
1	1	1	1	1	1	1	0	7
1	1	1	1	1	1	1	1	8



Distancia Hamming desde 0 hasta 255 y su correlato en potencia W

ANÁLISIS DE POTENCIA (SPA y DPA)

-Modelo de distancia Hamming dentro de una máquina de estados.

-Hipótesis 1: Hay corrrespondencia entre la potencia emitida (W_{leak}) y el número de "switches" de los bits.
-Hipótesis 2: $W_{leak}(0\text{-}1) = W_{leak}(1\text{-}0)$.
-Hipótesis 3: Todo el sistema está balanceado, es intemporal, y todos los bits son iguales (al menos localmente).

-$D=\sum d_j 2^j$ $\quad D=1*2^5+0*2^4+1*2^3+1*2^2+0*2^1+1*2^0 = 32+8+4+1 = 45$
-$H(D)=\sum d_j$ $\quad H(D)=1+0+1+1+0+1 = 4$

$j \in \{0,\ldots,m-1\}$

-Estadísticos
$\mu_H=m/2$
$\sigma^2_H=m/4$

ANÁLISIS DE POTENCIA (SPA y DPA)

-Modelo de distancia Hamming dentro de una máquina de estados.

- Número de bits cambiando de un estado al otro: $H(D_1 \oplus D_2)$.

-Hipótesis 4: Linealidad entre potencia y cambio de bits en un entorno local "caeteris paribus":

$$W=a* H(D_1 \oplus D_2)+b$$

-"b" incluye todas las variables independientes de nuestro cambio de bits, ruidos, offsets,…
-"a" es el factor de ganancia lineal.

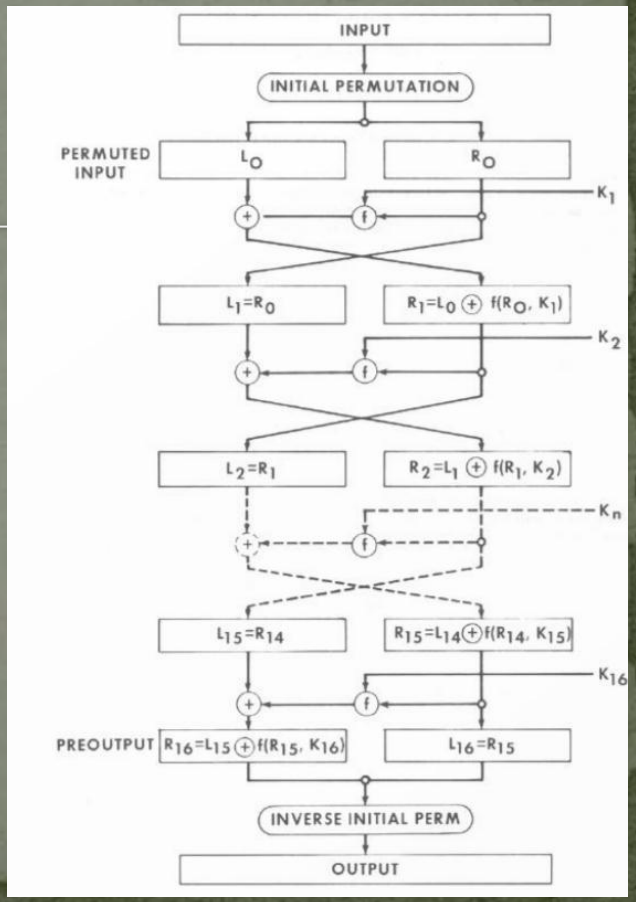
ANÁLISIS DE POTENCIA (SPA y DPA)

Atacando al cifrado DES:

Desde el original de 2^{56} opciones (72.057.594.037.927.936)

$+2^{45}$ (35.184.372.088.832) con SPA

$+2^{38}$ (274.877.906.944) con DPA.



SIMPLE POWER ANALYSIS (SPA)

-Observación directa del consumo de potencia.

-Dependencia del consumo con la instrucción realizada.

-Diferentes operaciones ofrecen diferente perfil de consumo.

-Análisis más detallados ofrecen datos de los valores a nivel de bit.

-Menos número de datos que DPA (más rápido en ejecutarse).

-No invasivo (o menos invasivo que DPA), aunque necesidad de herramientas de “microprobing”.

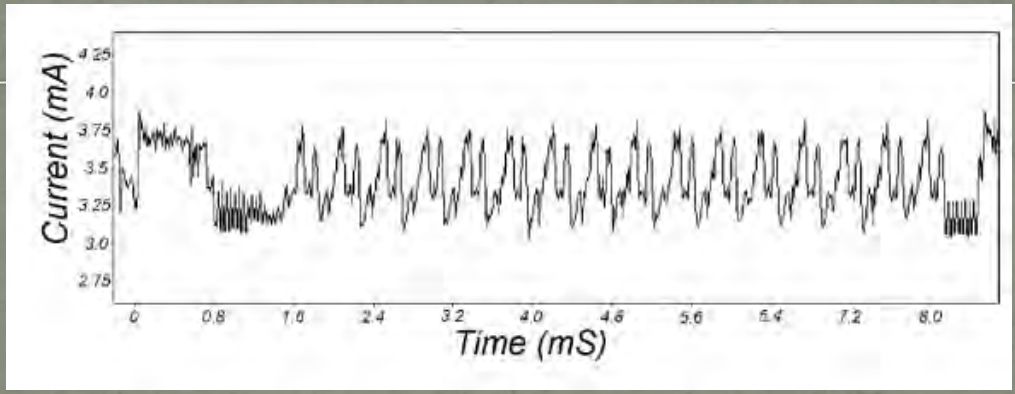
-Precisa de cierto conocimiento en la estructura y en el código que se está ejecutando.

-Los datos procesados son directamente proporcionales a las corrientes en el circuito y a la carga y descarga de las puertas lógicas.

SIMPLE POWER ANALYSIS (SPA)

Ataque al cifrador DES:

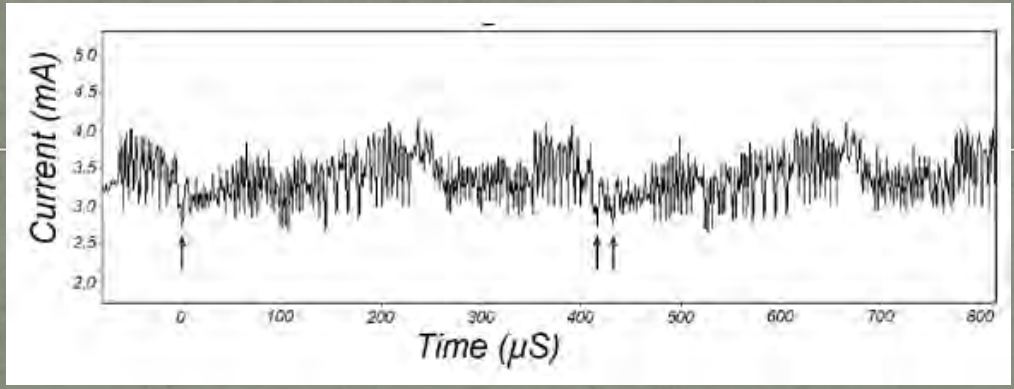
+Operación DES al completo:



SIMPLE POWER ANALYSIS (SPA)

Ataque al cifrador DES:

+Rondas 2 y 3:
(Rotaciones de las claves en la 2º ronda -1 vez-, y en la 3º ronda -2 veces.)

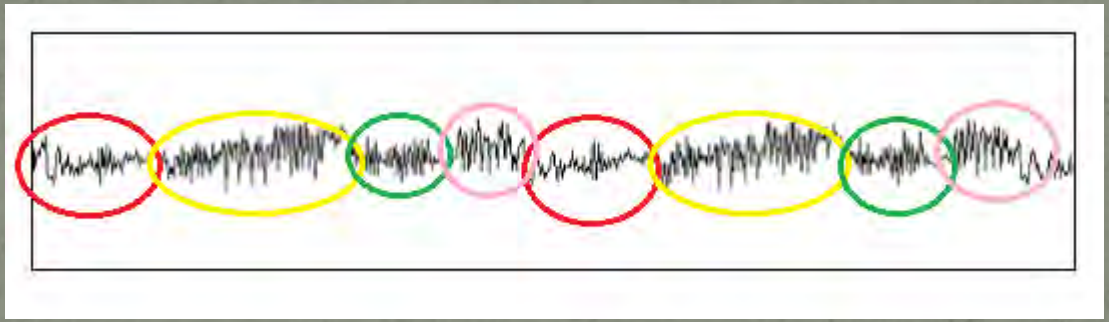


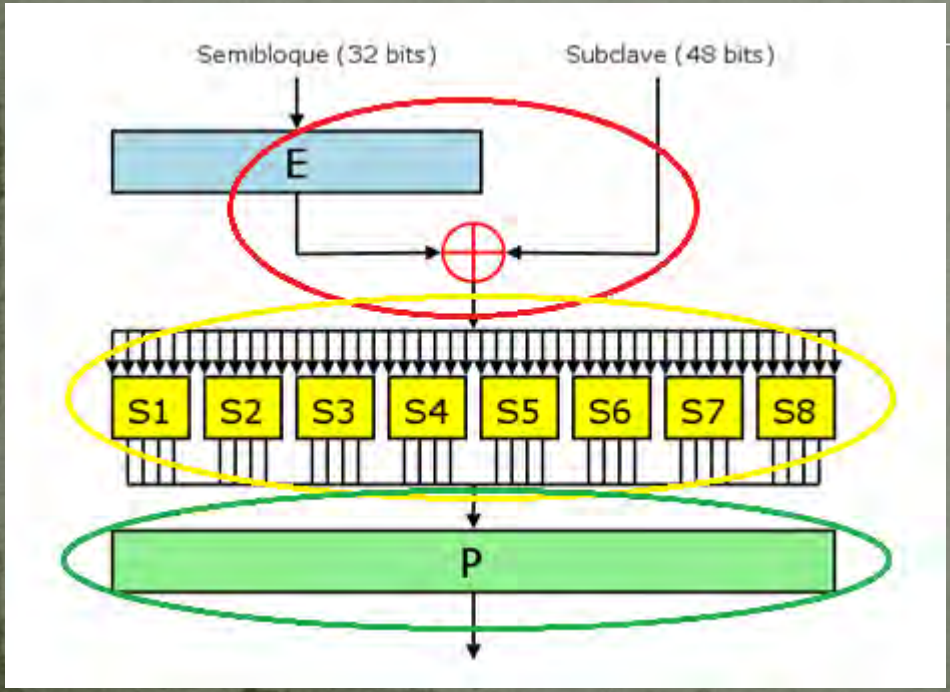
Subkey Rotation Table

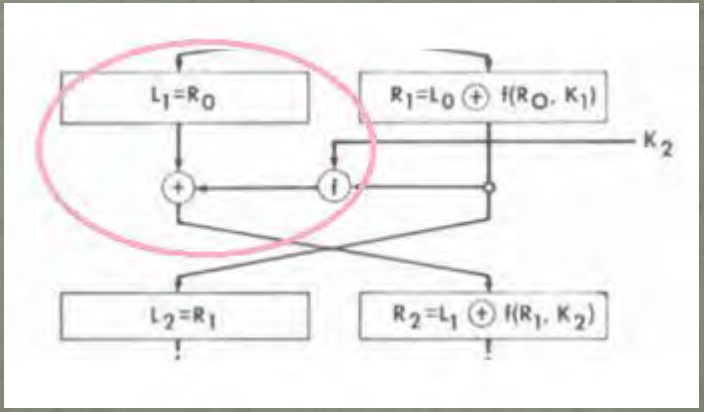
Round Number	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Number of bits to rotate	1	1	2	2	2	2	2	2	1	2	2	2	2	2	2	1

SIMPLE POWER ANALYSIS (SPA)

Ataque al cifrador DES: 2º y 3º round.





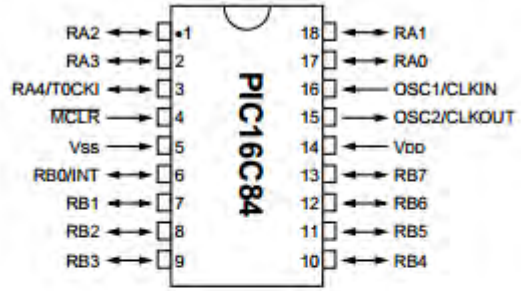


SIMPLE POWER ANALYSIS (SPA)

-Ejemplo de código:

Pin Diagram

PDIP, SOIC



CMOS Technology:

- Low-power, high-speed CMOS EEPROM technology
- Fully static design
- Wide operating voltage range:
  - Commercial: 2.0V to 6.0V
  - Industrial: 2.0V to 6.0V
- Low power consumption:
  - < 2 mA typical @ 5V, 4 MHz
  - 60 µA typical @ 2V, 32 kHz
  - 26 µA typical standby current @ 2V

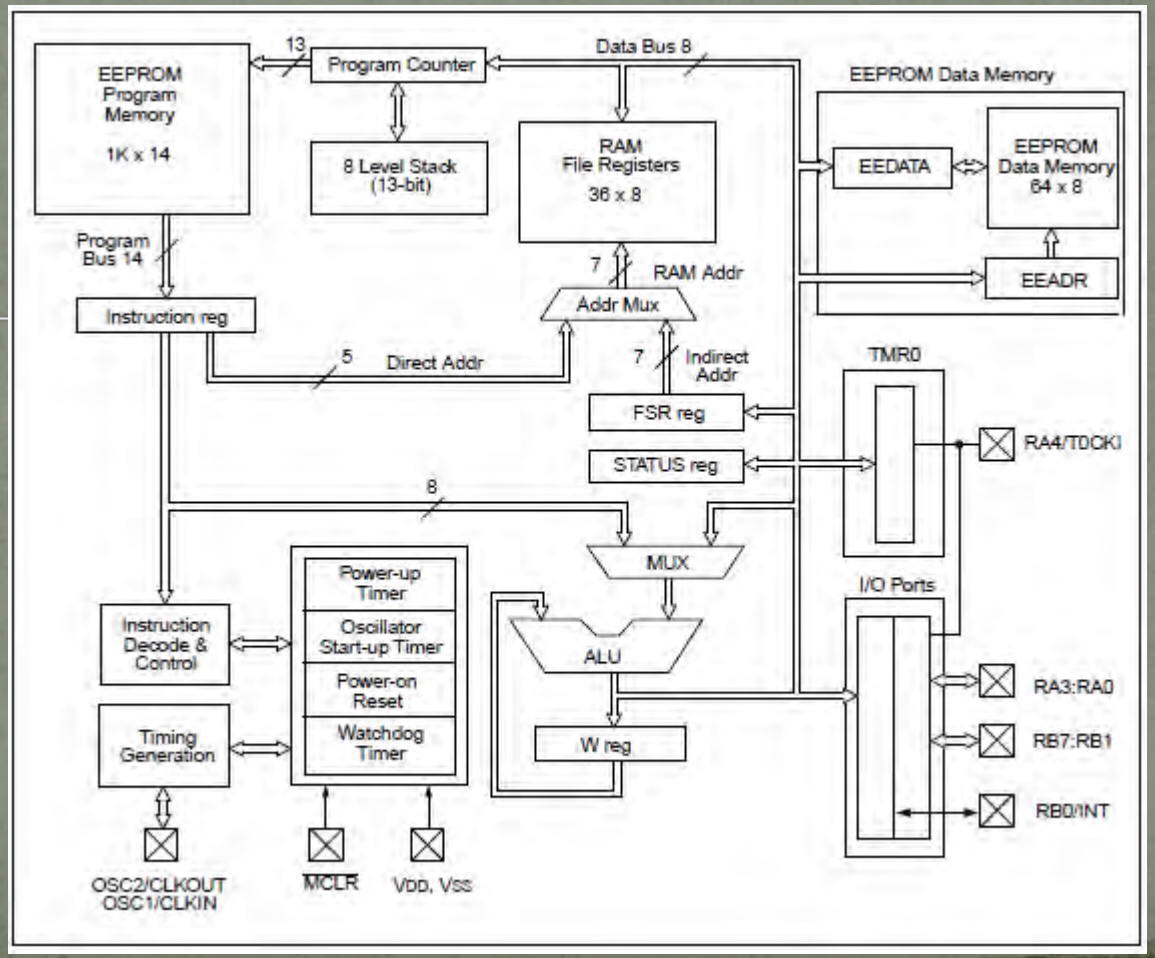
Pin Name	DIP No.	SOIC No.	I/O/P Type	Buffer Type	Description
OSC1/CLKIN	16	16	I	ST/CMOS (1)	Oscillator crystal input/external clock source input.
OSC2/CLKOUT	15	15	O	—	Oscillator crystal output. Connects to crystal or resonator in crystal oscillator mode. In RC mode, OSC2 pin outputs CLKOUT which has 1/4 the frequency of OSC1, and denotes the instruction cycle rate.
MCLR	4	4	I/P	ST	Master clear (reset) input/programming voltage input. This pin is an active low reset to the device.
					PORTA is a bi-directional I/O port.
RA0	17	17	I/O	TTL	
RA1	18	18	I/O	TTL	
RA2	1	1	I/O	TTL	
RA3	2	2	I/O	TTL	
RA4/T0CKI	3	3	I/O	ST	Can also be selected to be the clock input to the TMR0 timer/counter. Output is open drain type.
					PORTB is a bi-directional I/O port. PORTB can be software programmed for internal weak pull-up on all inputs.
RB0/INT	6	6	I/O	TTL	RB0/INT can also be selected as an external interrupt pin.
RB1	7	7	I/O	TTL	
RB2	8	8	I/O	TTL	
RB3	9	9	I/O	TTL	
RB4	10	10	I/O	TTL	Interrupt on change pin.
RB5	11	11	I/O	TTL	Interrupt on change pin.
RB6	12	12	I/O	TTL/ST (2)	Interrupt on change pin. Serial programming clock.
RB7	13	13	I/O	TTL/ST (2)	Interrupt on change pin. Serial programming data.
VSS	5	5	P	—	Ground reference for logic and I/O pins.
VDD	14	14	P	—	Positive supply for logic and I/O pins.

Legend: I= input O = output I/O = Input/Output P = power
— = Not used TTL = TTL input ST = Schmitt Trigger input

Note 1: This buffer is a Schmitt Trigger input when configured in RC oscillator mode and a CMOS input otherwise.
2: This buffer is a Schmitt Trigger input when used in serial programming mode.

SIMPLE POWER ANALYSIS (SPA)

-Ejemplo de código:



SIMPLE POWER ANALYSIS (SPA)

-Ejemplo de código:

+Esta variante, y otras:

-Descrecimientos (-1)
-Crecimientos (+3)
-Cambio de movwf REG por otras.

-Loop infinito.
-Escritura de números en REG desde 255 hasta 0.

```
; define registers VAL, PORTB, PORTA, REG:
VAL     equ 0x08
PORTA   equ 0x05
PORTB   equ 0x06            ; PORTA, PORTB:
REG     equ 0x0c  ;          output ports

start
        clrf    REG
        movlw   D'255'
        movwf   VAL         ; 0: move 255 to
 ; source value register

loopstart
        movfw   VAL, 0      ; 1: move new value to
        nop                 ; 2     accumulator
        nop                 ; 3
        movwf   REG         ; 4: ! move value from
        nop                 ; 5    accumulator to
        nop                 ; 6  internal register !
        movwf   PORTB       ; 7: move value to PORTB
        bsf     PORTA, 0    ; 8: set strobe bit
        bcf     PORTA, 0    ; 9: clear strobe bit
        clrf    PORTB       ;10: clear data in port B
        decfsz  VAL         ;11: decrease value, back
        goto    loopstart   ;12  to loopstart if !=0
        decf    VAL         ;13: set value to 255
        goto    start
```

SIMPLE POWER ANALYSIS (SPA)

-Ejemplo de código:

-Sampling 200 MHz (50 por ciclo).
-Probing con resistencia.
-Buscamos lugares de dependencia o correlación.

-Asunciones o hipótesis:

+Datos escritos en los registros.
+Datos escritos en el acumulador.

$$v_k = [v_k(0), v_k(1), \ldots, v_k(255)]$$

$$r_k = \frac{\sum_j (v_k(j) - \overline{v_k}) \cdot (p(j) - \overline{p})}{\sqrt{\sum_j (v_k(j) - \overline{v_k})^2} \cdot \sqrt{\sum_j (p(j) - \overline{p})^2}}$$

```
; define registers VAL, PORTB, PORTA, REG:
VAL     equ 0x08
PORTA   equ 0x05
PORTB   equ 0x06            ; PORTA, PORTB:
REG     equ 0x0c  ;          output ports

start
      clrf    REG
      movlw   D'255'
      movwf   VAL           ; 0: move 255 to
 ; source value register

loopstart
      movfw   VAL, 0        ; 1: move new value to
      nop                   ; 2     accumulator
      nop                   ; 3
      movwf   REG           ; 4: ! move value from
      nop                   ; 5    accumulator to
      nop                   ; 6  internal register !
      movwf   PORTB         ; 7: move value to PORTB
      bsf     PORTA, 0      ; 8: set strobe bit
      bcf     PORTA, 0      ; 9: clear strobe bit
      clrf    PORTB         ;10: clear data in port B
      decfsz  VAL           ;11: decrease value, back
      goto    loopstart     ;12  to loopstart if !=0
      decf    VAL           ;13: set value to 255
      goto    start
```

SIMPLE POWER ANALYSIS (SPA)

-Ejemplo de código:

+Análisis de los pesos Hamming, transiciones, valores de los datos, almacenamientos,…

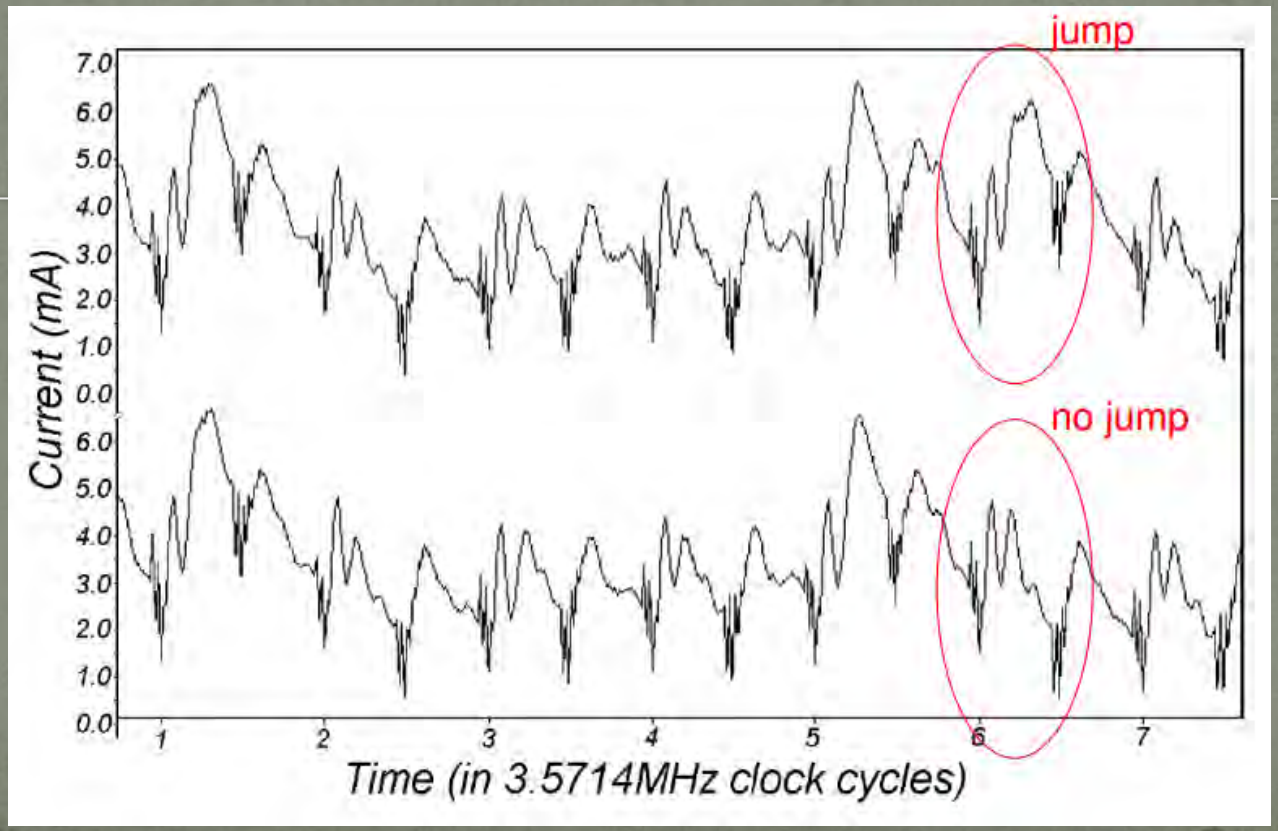
+Las instrucciones ofrecen información, incluso un “mov”, “subwf”, xorwf”, y los datos asociados y desplazados por los buses.

+Existe control de la frecuencia y del voltaje, es decir de la “capacidad” (nos permite ajustes finos y evitar señales de ruido).

SIMPLE POWER ANALYSIS (SPA)

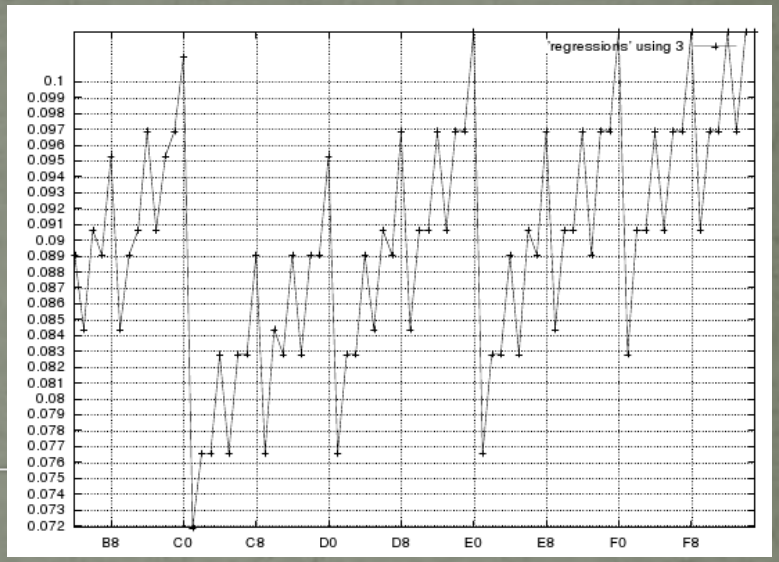
-Ejemplo de código:

+Diferencias de consumo según se produzca el salto en una instrucción “jump”.

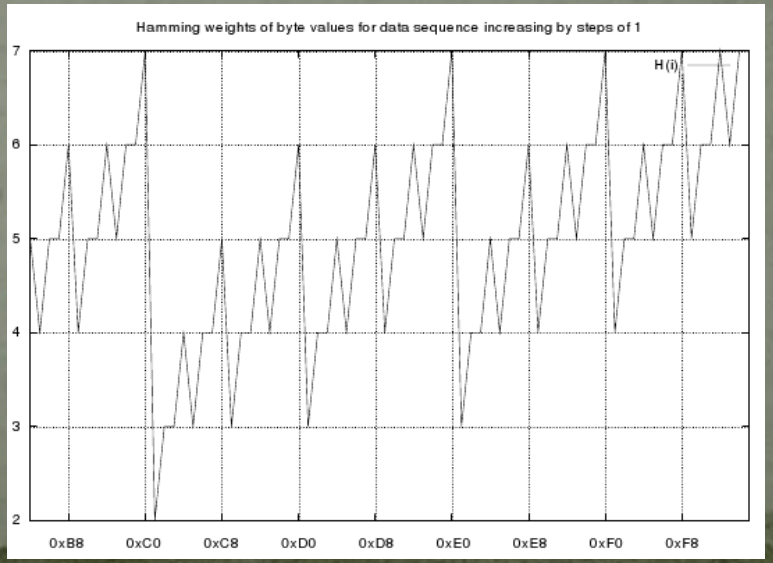


SIMPLE POWER ANALYSIS (SPA)

-Ejemplo de código:

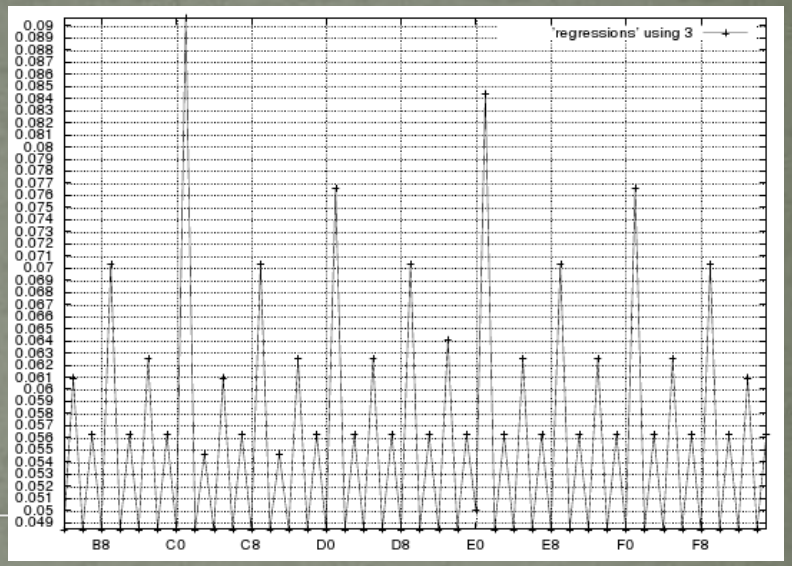


+ Medidas de voltaje correladas al peso De Hamming con datos desde 180 a 256 en la transferencia de datos.

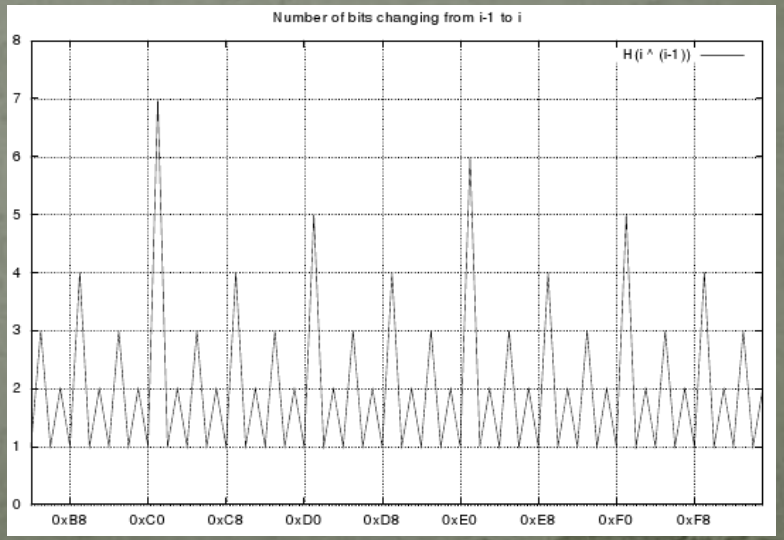


SIMPLE POWER ANALYSIS (SPA)

-Ejemplo de código:



+ Medidas de voltaje correladas al peso De Hamming con datos desde 180 a 256 en la transición de cuenta.



SIMPLE POWER ANALYSIS (SPA)

-Ataque a RSA:

+Algoritmo de exponenciación (forma habitual): "Square and Multiply (SM)"

$x^{SK}=x^{314}$

$314_{(10}=100111010_{(2}$

1	0	0	1	1	1	0	1	0
x^1	x^2	x^4	x^9	x^{19}	x^{39}	x^{78}	x^{157}	x^{314}

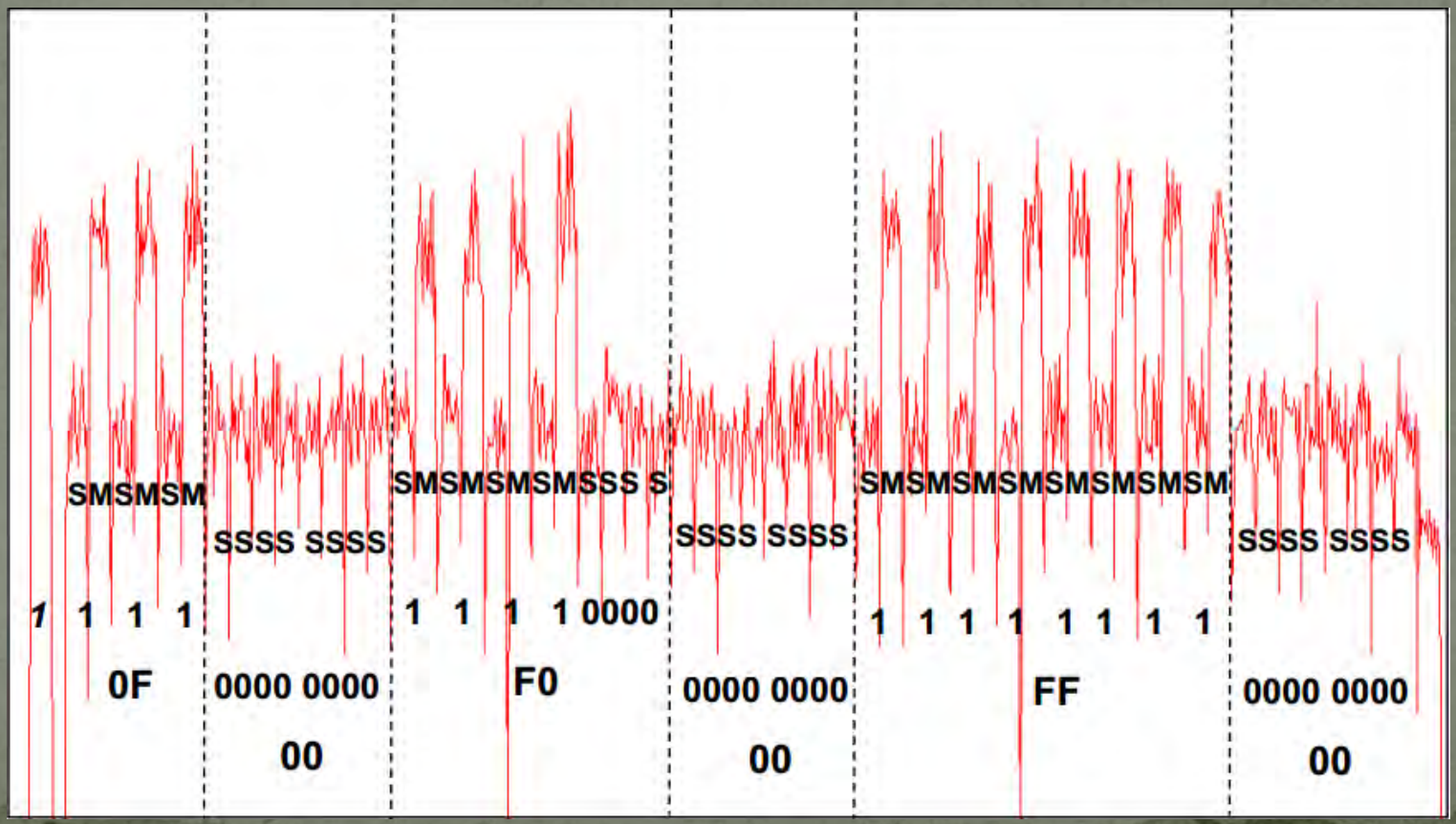
$k \leftarrow \text{bitsize}(d)$
$y \leftarrow x$
for $i = k - 2$ **downto** 0 **do**
  $y \leftarrow y^2 \pmod n$
  if (bit i of d is 1) **then** $y \leftarrow y \cdot x \pmod n$
endfor
return y

+Una exponencial de la que queremos conocer el exponente (SK) es en definitiva un doblado de valor y un producto "de vez en cuando".

SIMPLE POWER ANALYSIS (SPA)

-Ataque a RSA:

+Algoritmo de exponenciación (forma habitual): “Square and Multiply (SM)”
+Veamos una key de test: 0F00F000FF00

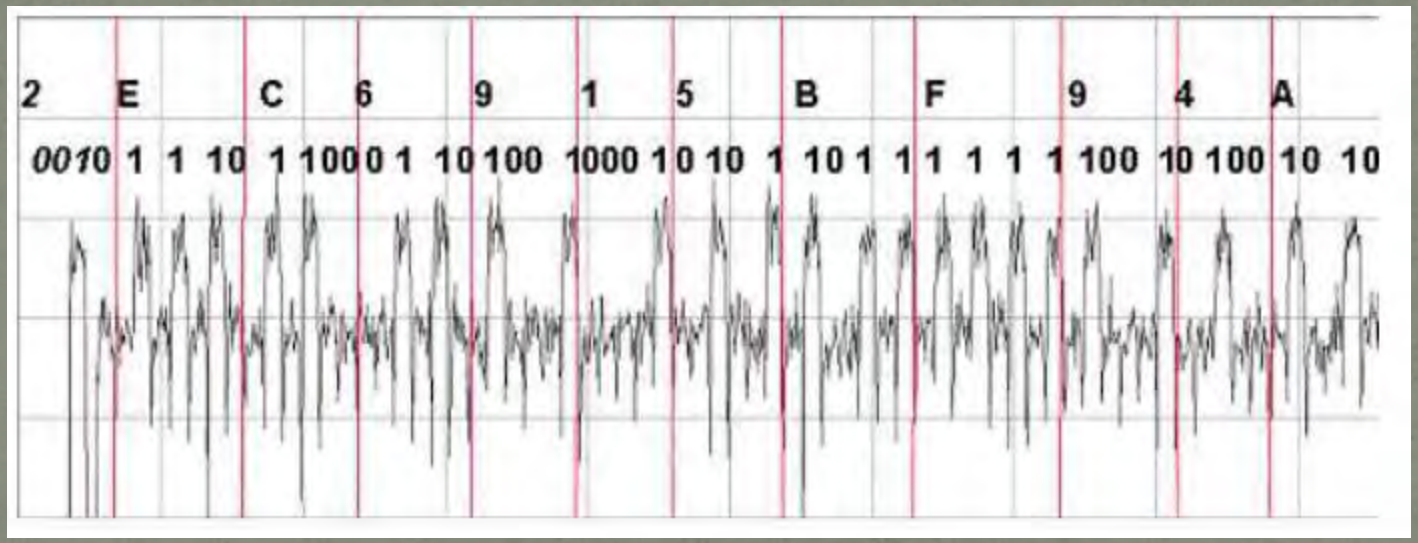


SIMPLE POWER ANALYSIS (SPA)

-Ataque a RSA:

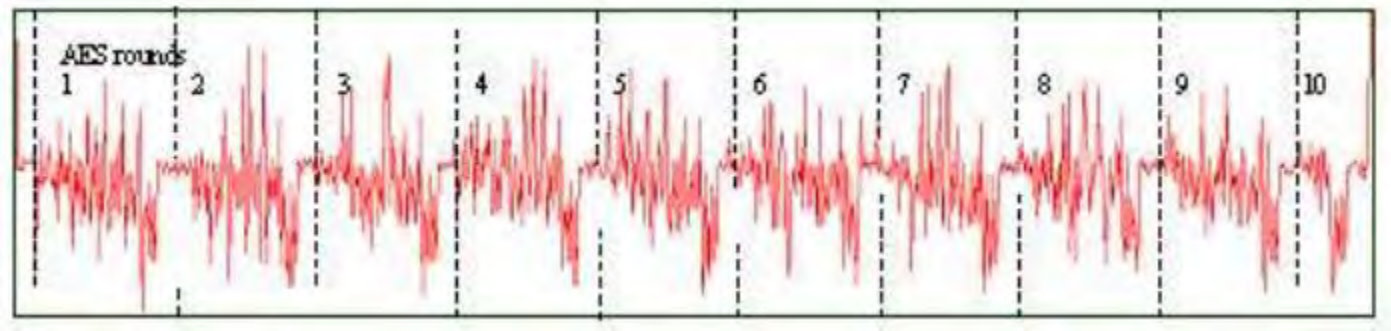
+Algoritmo de exponenciación (forma habitual): “Square and Multiply (SM)”

+Veamos ahora la clave que buscamos:



SIMPLE POWER ANALYSIS (SPA)

-Pasa igual con los demás cifrados: AES



+Futuras especificaciones: dar mayor importancia a side-channel que hasta ahora para la elección de los candidatos.

DIFFERENTIAL POWER ANALYSIS (DPA)

-Más potente que SPA.

-Más difícil de prevenir.

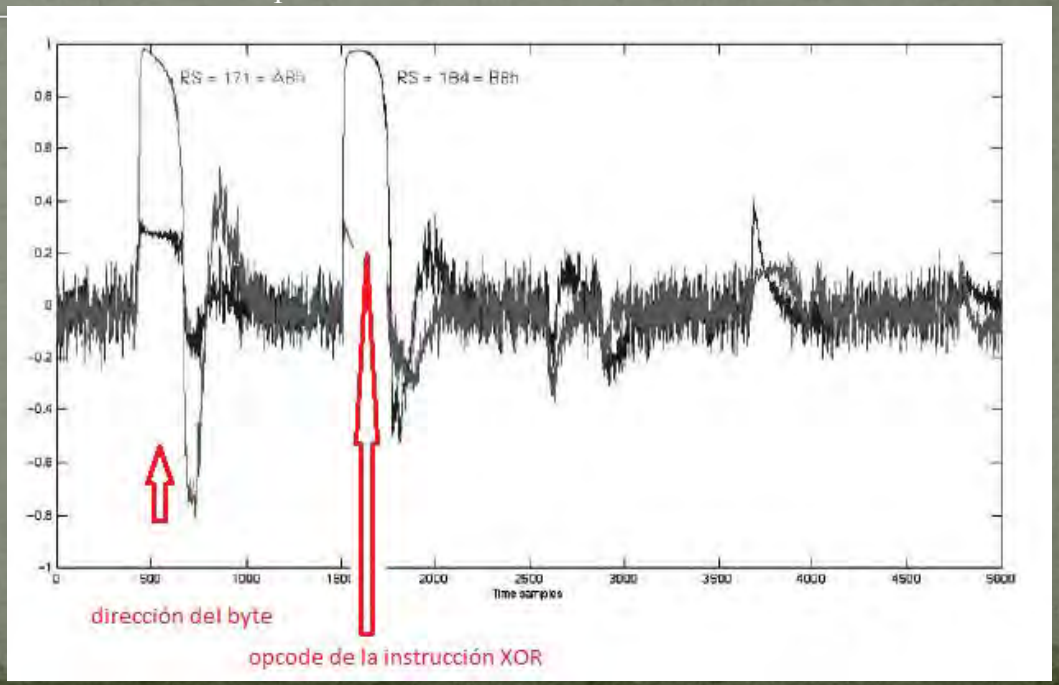
-En muchas características es opuesto a SPA en sus contramedidas.

-Dos fases: Recolección de datos y Análisis estadístico con técnicas de corrección de errores (Hamming) y correlación.

DIFFERENTIAL POWER ANALYSIS (DPA)

Experimento:

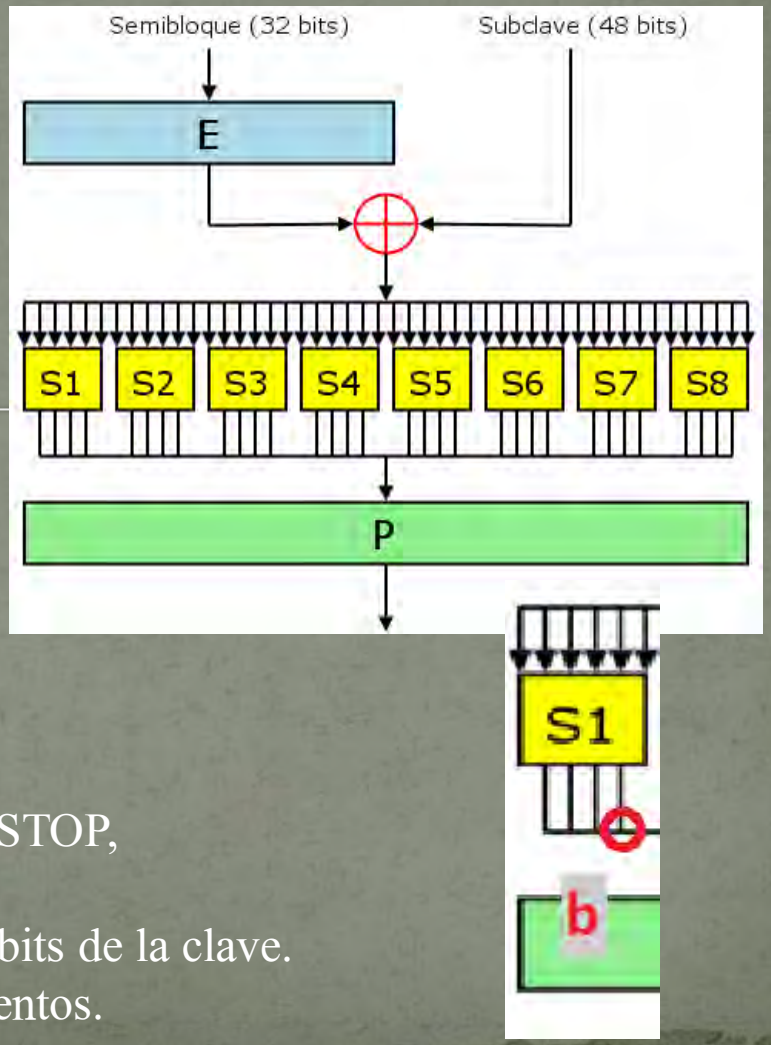
-Chip de 8 bits, operación XOR.
-d_2 es una constante.
-LOAD byte d_1
-$d_1 \oplus d_2$
-Guardamos el resultado desde el acumulador a un destino en memoria.
-Realización 256 veces, con variaciones de d_1 desde 0 a 256.



DIFFERENTIAL POWER ANALYSIS (DPA)

-Ataque cifrado DES:

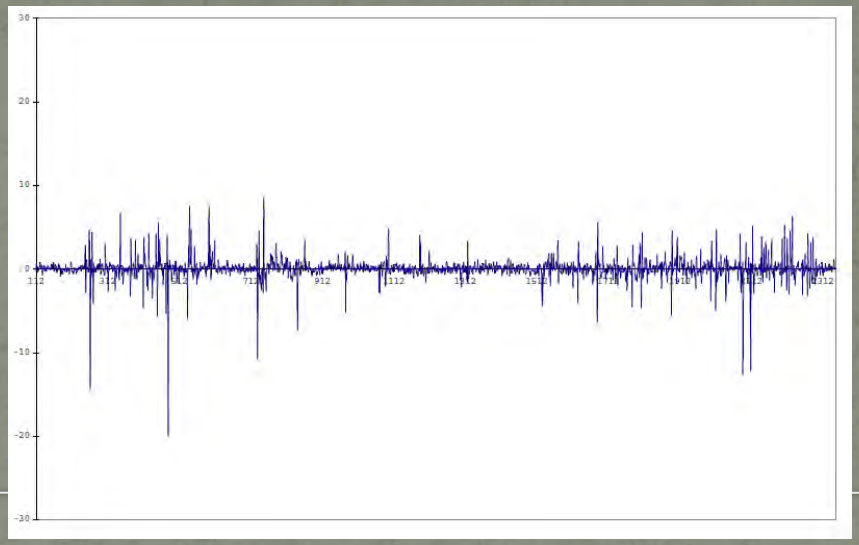
-16 rondas.
-Transformación f.
-S-box.



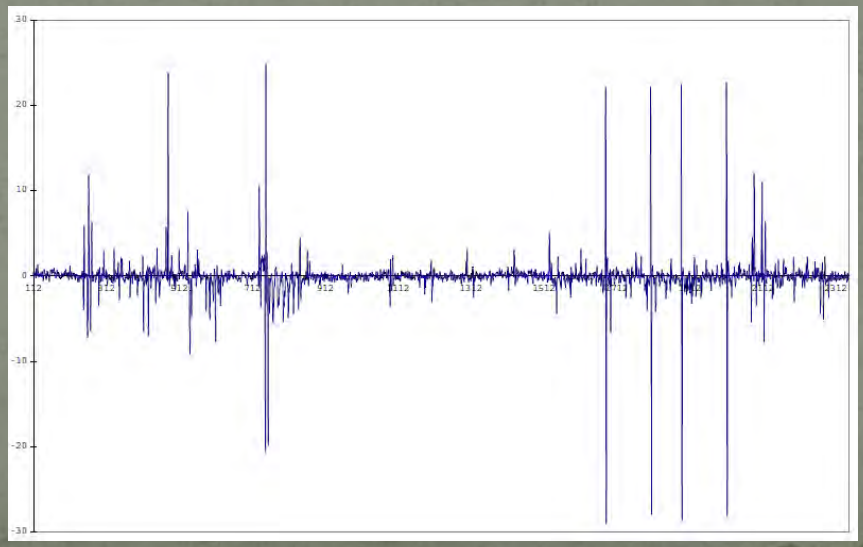
+Experimento: 1000 veces.
+1º ronda.
+Entradas $E=\{E_1,\ldots,E_{1000}\}$.
+Curvas de consumo $C=\{C_1,\ldots,C_{1000}\}$.
+Curva media MC de cada 1000.
+Bit "b" de S-box 1 (dependiente de 6 bits).
+Partición de E / b=0, b=1.
+$MC_{,/b=0}$ (¿correlación?): Si son "distintos" STOP, "else", otra combinación de 6 bits: $2^6=64$.
+Igual en 2º ronda, 3º ronda… 8º ronda: 48 bits de la clave.
+Resto de bits (8), por ataque bruto: 256 intentos.

DIFFERENTIAL POWER ANALYSIS (DPA)

-Ataque cifrado DES:



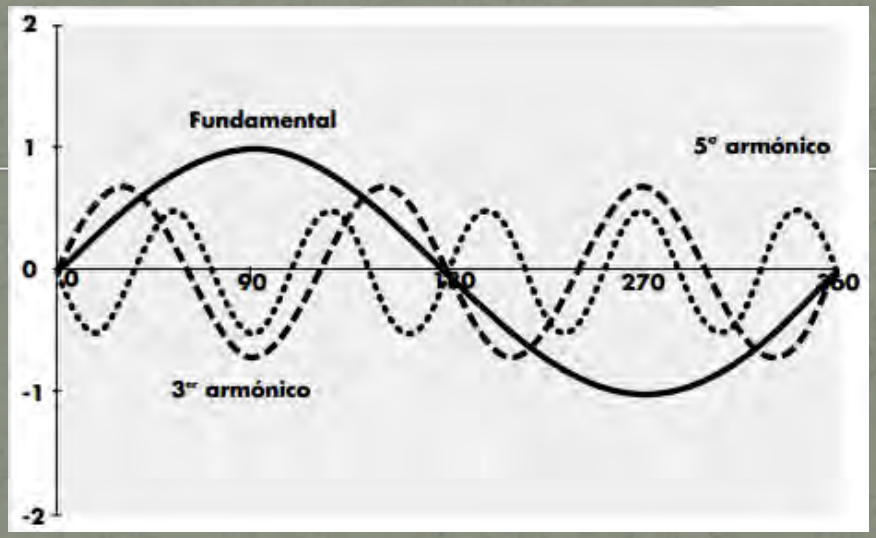
¡Sigue intentándolo!



¡Eureka!

ANÁLISIS ELECTROMAGNÉTICO (SEMA y DEMA)

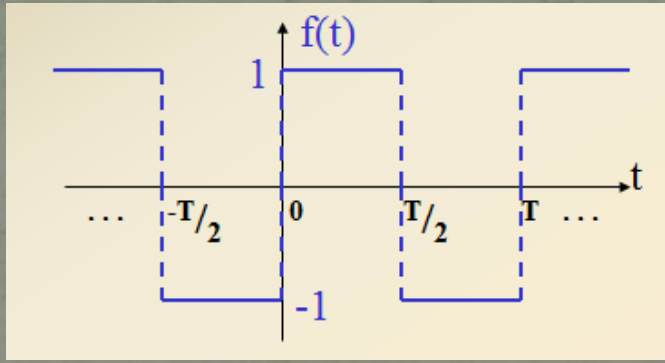
-Una historia antigua pero en parte desconocida (TEMPEST).
-Muy ligado al anterior (análisis de potencia).
-Muy similar en sus herramientas.
-En algunos casos puede ser complementario al de potencia.
-Cuidado con las contramedidas entre ambos pues no tienen por qué solaparse.



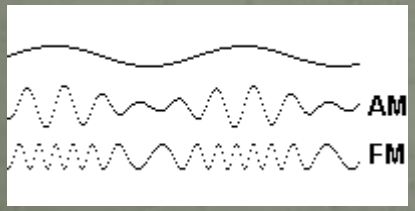
-SEMA (Simple ElectroMagnetic Attack) es a SPA, como DEMA (Differential ElectroMagnetic Attack) es a DPA.

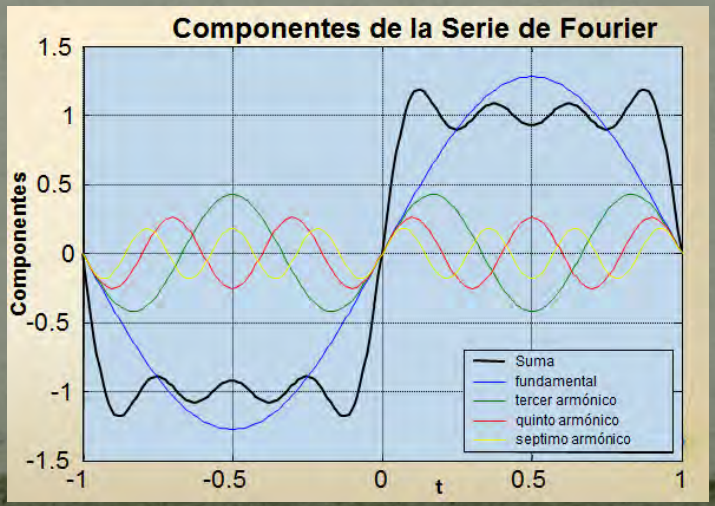
ANÁLISIS ELECTROMAGNÉTICO (SEMA y DEMA)

-Frecuencia fundamental y los armónicos como frecuencias “leakage”.



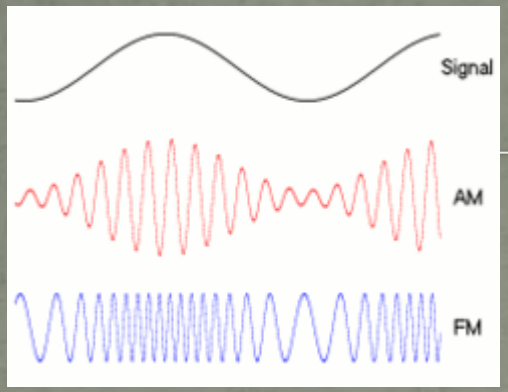
$$f(t) = \frac{4}{\pi}\left[\operatorname{sen}(\omega_0 t) + \tfrac{1}{3}\operatorname{sen}(3\omega_0 t) + \tfrac{1}{5}\operatorname{sen}(5\omega_0 t) + \ldots\right]$$

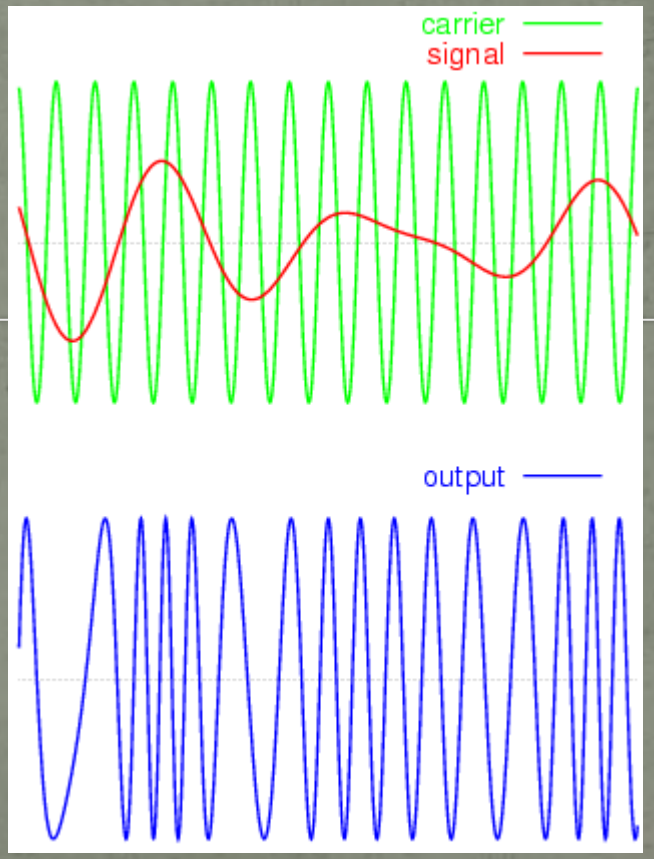




ANÁLISIS ELECTROMAGNÉTICO (SEMA y DEMA)

-Demodulando los datos capturados con una antena para sacar la señal.



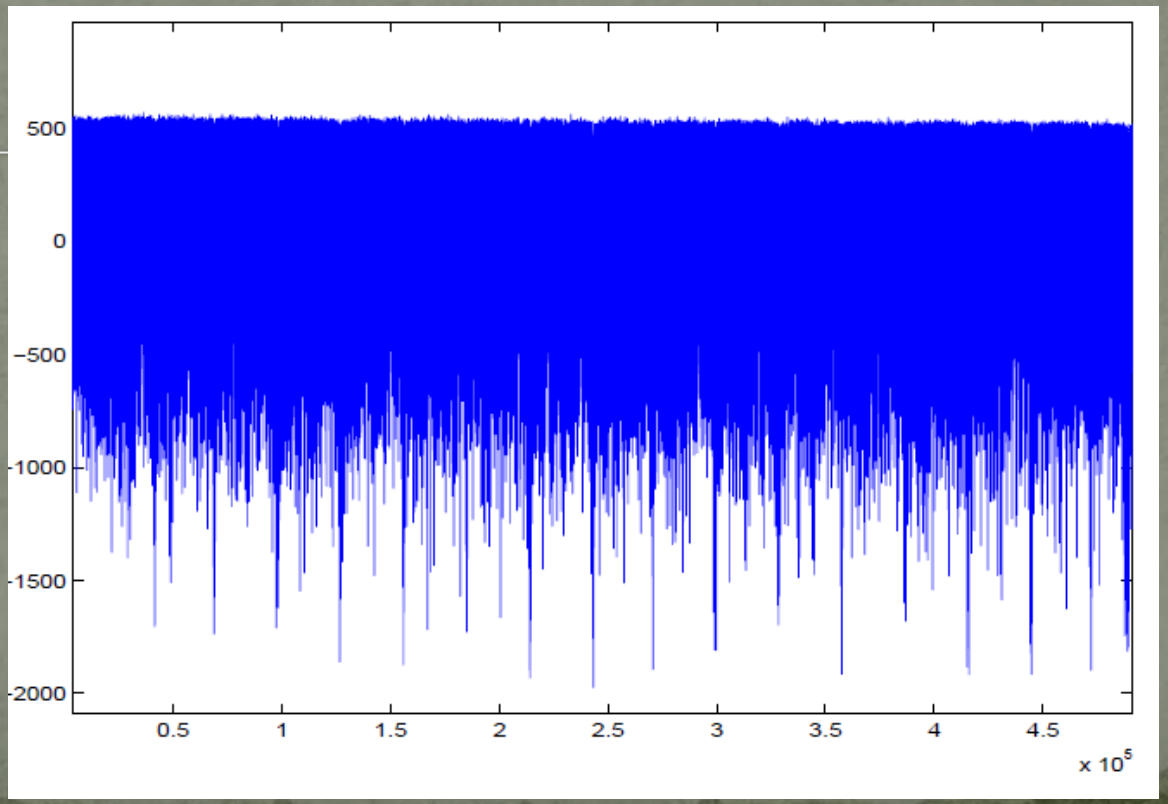


-El resto de material de trabajo (instrumentación) es similar al ataque de potencia.

SIMPLE ELECTROMAGNETIC ATTACK (SEMA)

Ataque al cifrador DES:

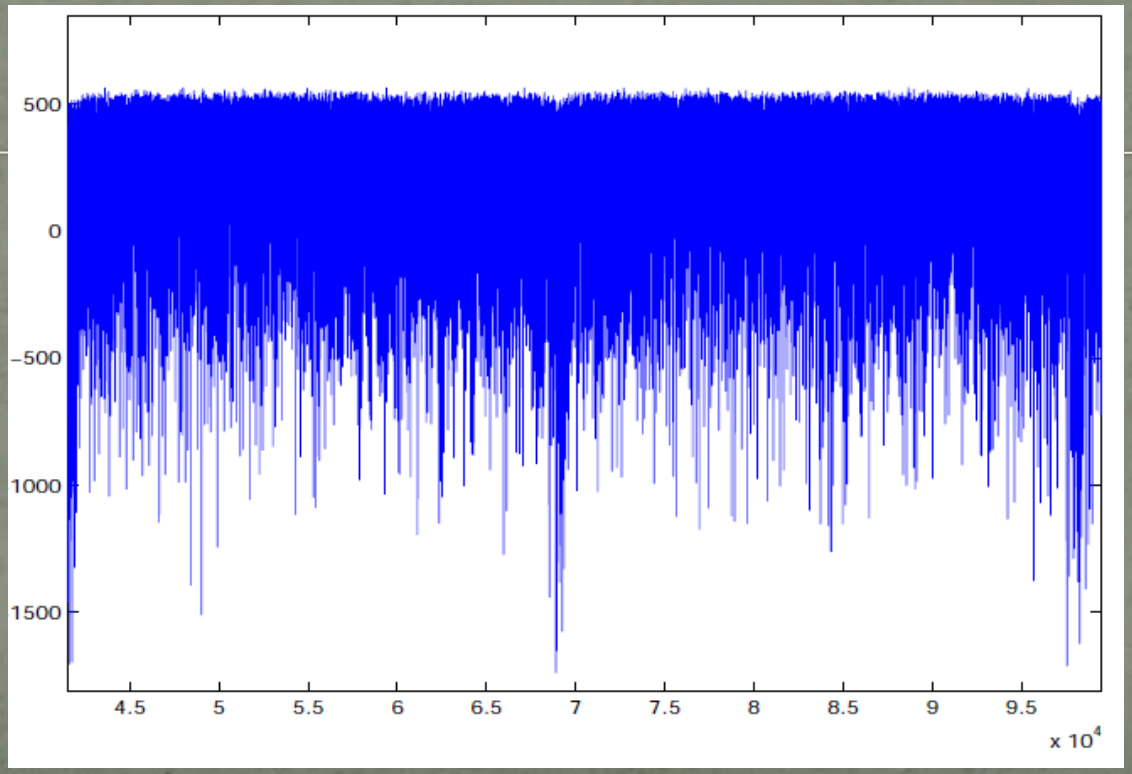
+Operación DES al completo:



SIMPLE ELECTROMAGNETIC ATTACK (SEMA)

Ataque al cifrador DES:

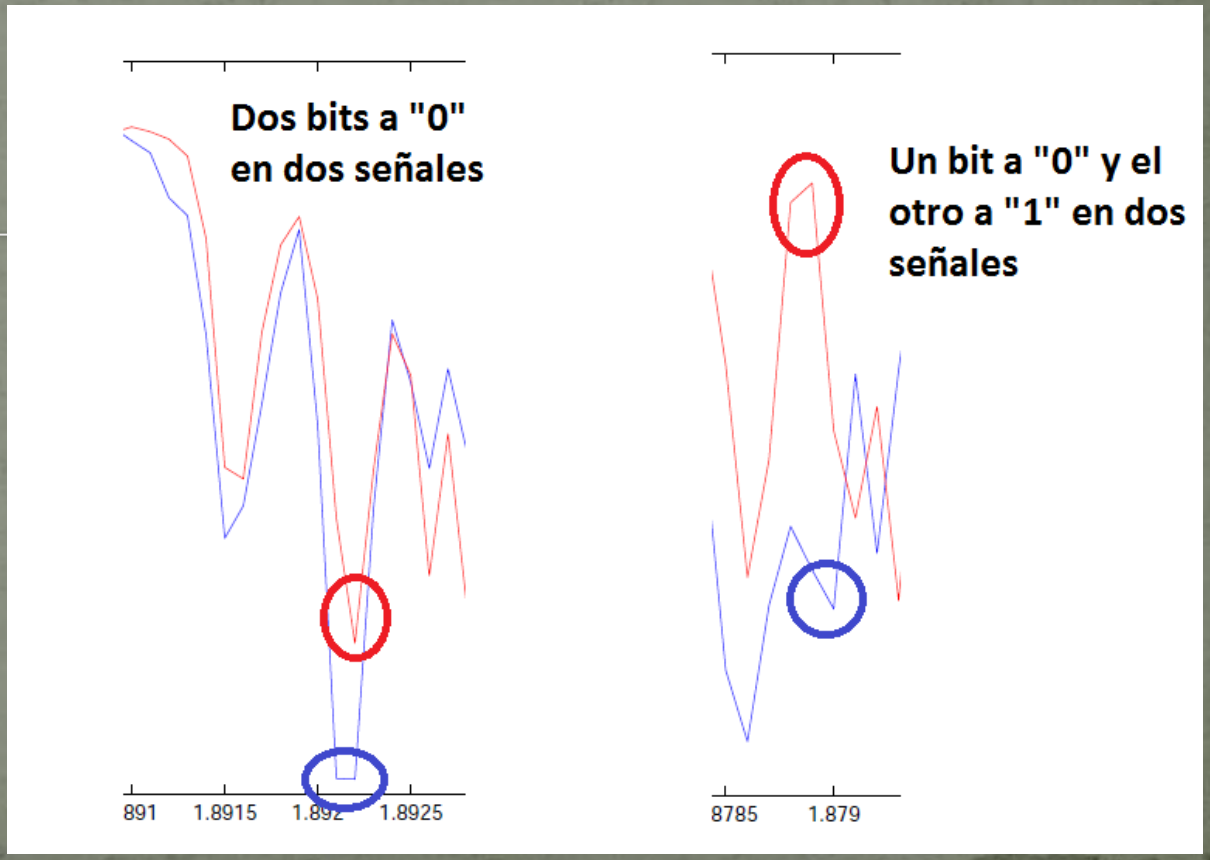
+Operación DES (2 rondas):



SIMPLE ELECTROMAGNETIC ATTACK (SEMA)

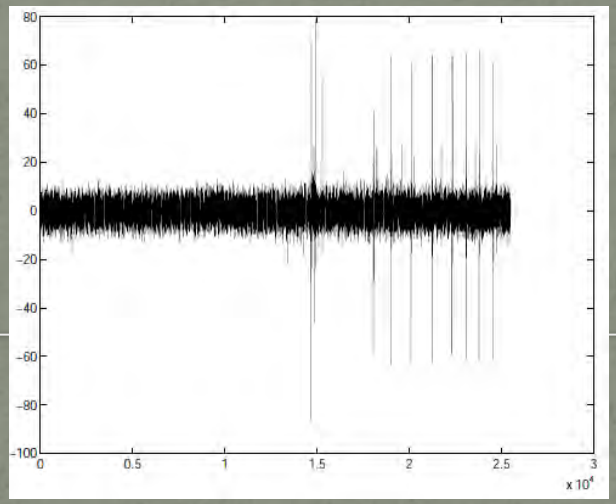
Ataque al cifrador DES:

+Diferencias a nivel de bit:

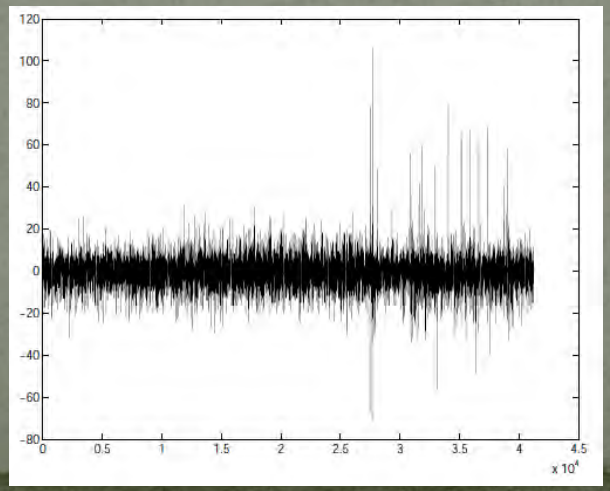


DIFFERENTIAL SIMPLE ELECTROMAGNETIC ATTACK (DEMA)

-Ataque cifrado DES:



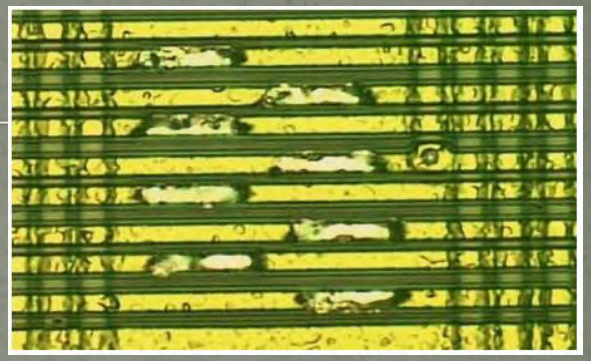
¡Eureka! (DPA)



¡Eureka! (DEMA)

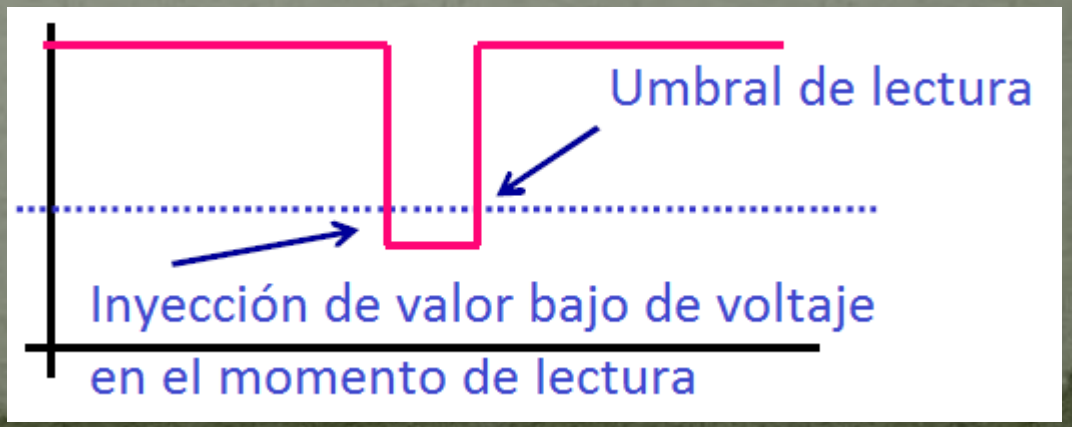
INYECCIÓN DE ERRORES

+ Cambio de los valores de lectura o escritura: memoria, bus, registros… (distintas instrucciones se ejecutan, distintos valores van por el bus a pesar de las salidas reales, …).
+Ejemplo sobre el cambio de una instrucción: transformamos un cifrado de "n" rondas en uno de una sola ronda.
+ Muy potentes.



Ejemplo:

-Manipulación del voltaje.
-Pulsos electromagnéticos.
-Rayos luminosos.
-Temperatura
-etc.



INYECCIÓN DE ERRORES

+ Algunas técnicas:

(a) Ataques al clock:
Los más simples y comunes. Aumento de f_{CLK} (1 ó más ciclos) para "samplear" en otro momento.

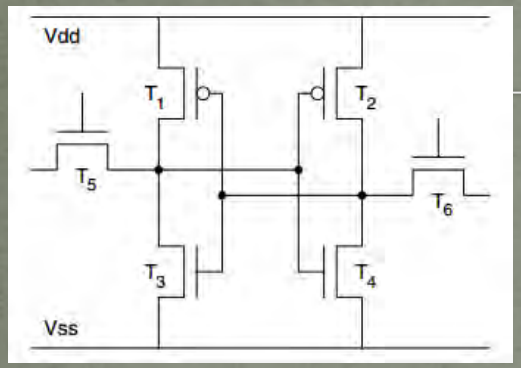
(b) Transiciones de potencia:
"Glitches" o "shiftings".

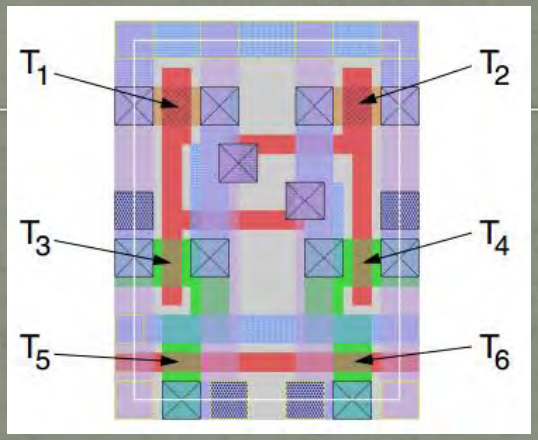
(c) Transiciones de voltaje:
Inserción de puentes de voltaje con metalizaciones en los extremos en zonas de movimiento iónico de transistores.

INYECCIÓN DE ERRORES

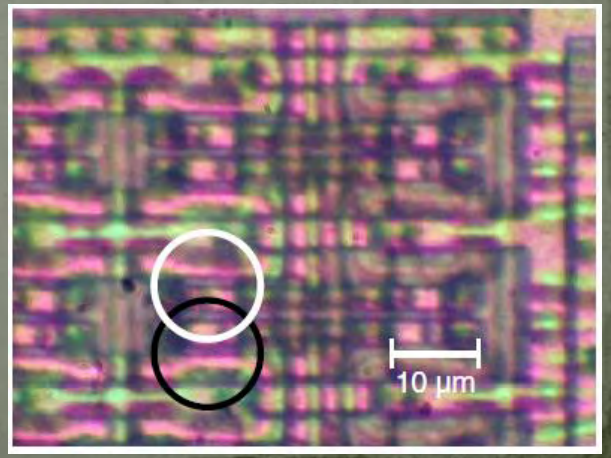
(b) Transiciones de potencia:

-Memoria SRAM.
-Uso de luz para cambiar los estados:





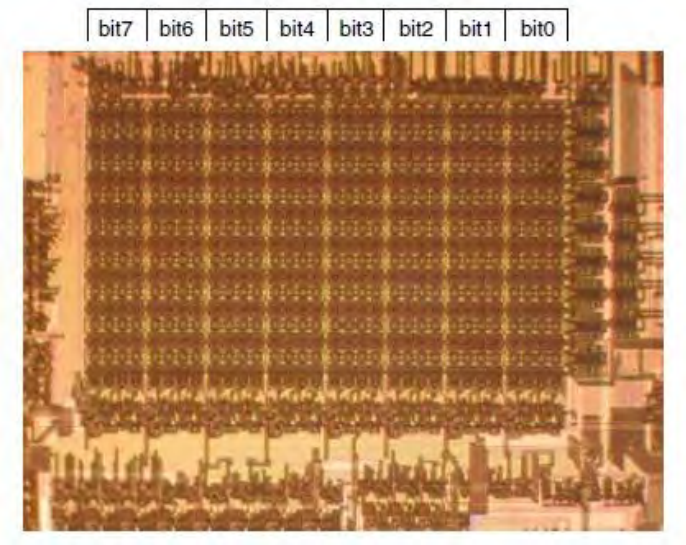
Zona blanca: Obliga a “0”
Zona negra: Obliga a “1”



INYECCIÓN DE ERRORES

(b) Transiciones de potencia:

-Memoria SRAM: mapeo de direcciones.



30h	34h	38h	3Ch	40h	44h	48h	4Ch	10h	14h	18h	1Ch	20h	24h	28h	2Ch	0Ch
31h	35h	39h	3Dh	41h	45h	49h	4Dh	11h	15h	19h	1Dh	21h	25h	29h	2Dh	0Dh
32h	36h	3Ah	3Eh	42h	46h	4Ah	4Eh	12h	16h	1Ah	1Eh	22h	26h	2Ah	2Eh	0Eh
33h	37h	3Bh	3Fh	43h	47h	4Bh	4Fh	13h	17h	1Bh	1Fh	23h	27h	2Bh	2Fh	0Fh

ATAQUES TEMPORALES

-Distintas tareas con distintas herramientas conllevan distinto tiempo de ejecución.

-Saltos, condiciones, operaciones matemáticas, finales de “loop”, cachés, paralelizaciones, coprocesadores,…

ATAQUES TEMPORALES

Ataque al cifrador RSA:

"*By carefully measuring the amount of time required to perform private key operations, attackers may be able to find fixed Diffie-Hellman exponents, factor RSA keys, and break other cryptosystems.*" (Paul C. Kocher)

$x^{SK}=x^{314}$

$314_{(10}=100111010_{(2}$

1	0	0	1	1	1	0	1	0
x^1	x^2	x^4	x^9	x^{19}	x^{39}	x^{78}	x^{157}	x^{314}

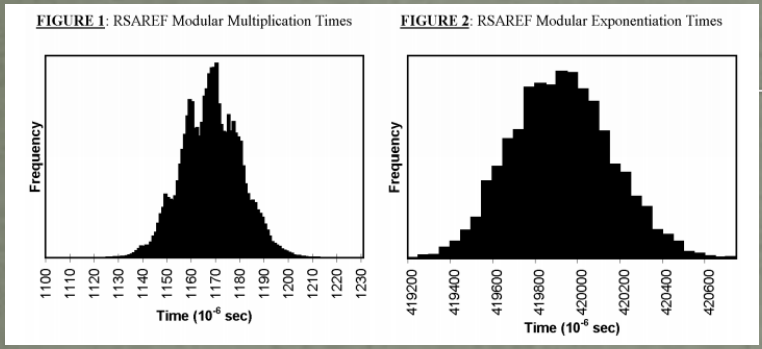
$k \leftarrow \text{bitsize}(d)$
$y \leftarrow x$
for $i = k - 2$ **downto** 0 **do**
  $y \leftarrow y^2 \pmod n$
  if (bit i of d is 1) **then** $y \leftarrow y \cdot x \pmod n$
endfor
return y

ATAQUES TEMPORALES

Ataque al cifrador RSA:

1	0	0	1	1	1	0	1	0
x^1	x^2	x^4	x^9	x^{19}	x^{39}	x^{78}	x^{157}	x^{314}

$k \leftarrow \text{bitsize}(d)$
$y \leftarrow x$
for $i = k - 2$ **downto** 0 **do**
  $y \leftarrow y^2 \pmod n$
  if (bit i of d is 1) **then** $y \leftarrow y \cdot x \pmod n$
endfor
return y



$$P(x_b) \propto \prod_{i=0}^{j-1} F(T_i - t(y_i, x_b))$$

-/Exp/Exp/Exp+Mul/Exp+Mul/Exp+Mul/Exp/Exp+Mul/Exp/

-8 Exp y 4 Mul: 9 bits

-1-?-?-?-?-?-?-?-?

ALGUNAS PALABRAS QUE A VECES ESCUCHAMOS

-Ataques TEMPEST, TEAPOT, HIJACK, NONSTOP, …

~~SECRET~~

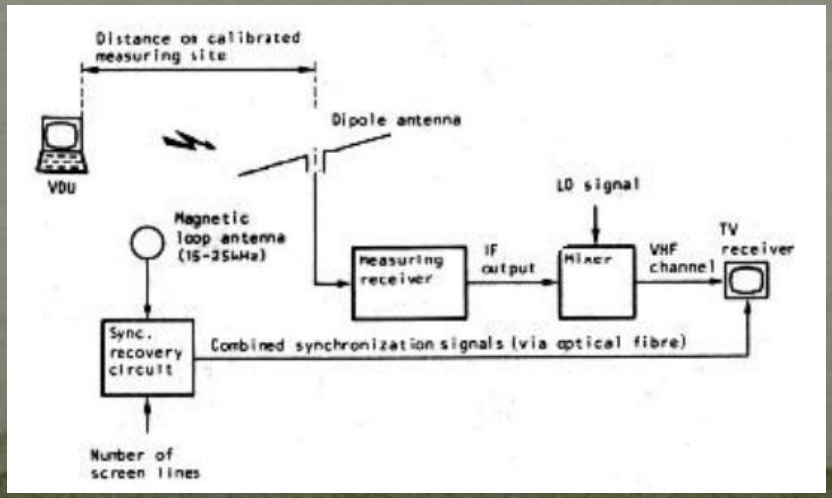
Approved for Release by NSA on 09-27-2007, FOIA Case # 51633

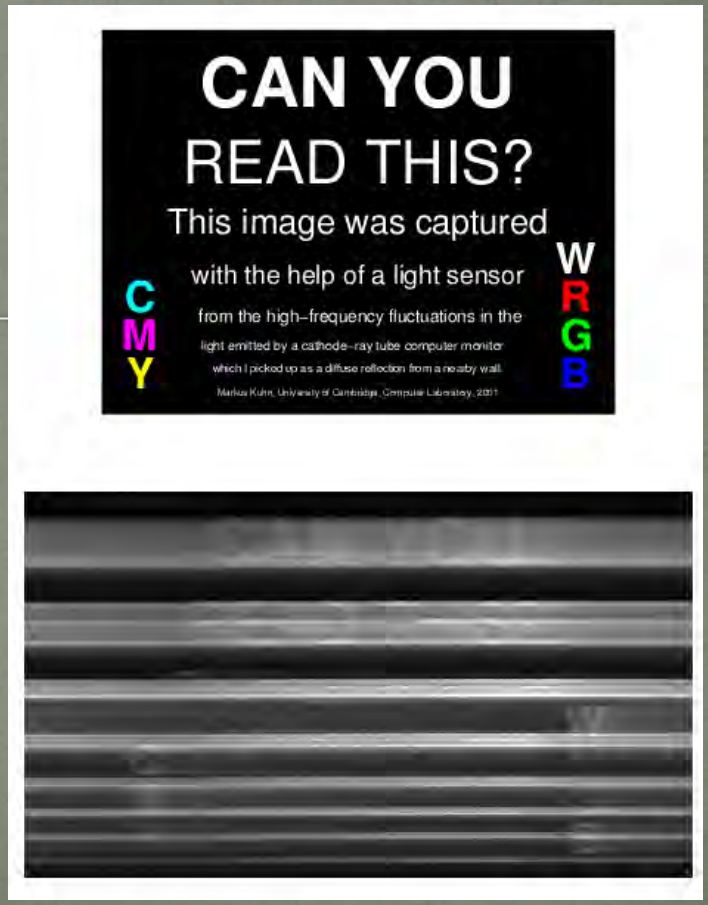
TEMPEST: A Signal Problem

The story of the discovery of various compromising radiations from communications and Comsec equipment.

In 1962, an officer assigned to a very small intelligence detachment in Japan was performing the routine duty of inspecting the area around his little cryptocenter. As required, he was examining a zone 200 ft. in radius to see if there was any "clandestine technical surveillance." Across the street, perhaps a hundred feet away, was a hospital controlled by the Japanese government. He sauntered past a kind of carport jutting out from one side of the building and, up under the eaves, noticed a peculiar thing—a carefully concealed dipole antenna, horizontally polarized, with wires leading through the solid cinderblock wall to which the carport abutted. He moseyed back to his headquarters, then quickly notified the counter-intelligence people and fired off a report of this "find" to Army Security Agency, who, in turn, notified NSA. He was directed to examine this antenna in detail and perhaps secure it, but found with microphones for? Why was there a large metal grid carefully buried in the cement of the ceiling over the Department of State communications area? A grid with a wire leading off somewhere. And what was the purpose of the wire that terminated in a very fine mesh of smaller hair-like wires? And, while we were at it, how did these finds relate to other mysterious finds and reports from behind the Curtain—reports dating clear back to 1953?

Why, way back in 1954, when the Soviets published a rather comprehensive set of standards for the suppression of radio frequency interference, were those standards much more stringent for their teletypewriters and other communications equipment than for such things as diathermy machines, industrial motors, and the like, even though the teletypewriters were much quieter in the first





ESTOS ATAQUES NO SON TAN NOVEDOSOS EN SÍ MISMOS...

+Presión ejercida al escribir y marcada en la hoja inferior.

ESTOS ATAQUES NO SON TAN NOVEDOSOS EN SÍ MISMOS…

-Sonido como canal lateral de lo que ocurre:

ESTOS ATAQUES NO SON TAN NOVEDOSOS EN SÍ MISMOS...

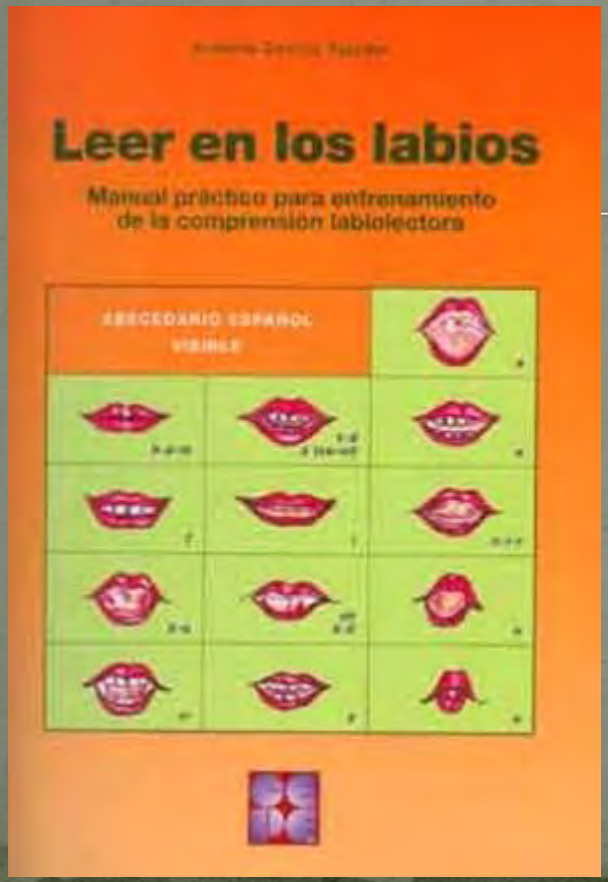
-Sonido como canal lateral:

+Atenuación por la distancia.
+Absorción por el aire (u otro medio) -dependiente de la frecuencia, temperatura, humedad del medio...
+Influencia del viento (curvatura del sonido), obstáculos y absorciones, reflexiones, difracciones, efectos del suelo,…

Solución: Acercarse para evitar disminuir la potencia emitida, enmascarar con ruido (música), etc..

ESTOS ATAQUES NO SON TAN NOVEDOSOS EN SÍ MISMOS...

- Y en el caso del uso visual para conocer las palabras:



ESTOS ATAQUES NO SON TAN NOVEDOSOS EN SÍ MISMOS...

-"Lectura fría" en la lectura de cartas (todo un ataque lateral).

ESTOS ATAQUES NO SON TAN NOVEDOSOS EN SÍ MISMOS...

-Arquímedes, Hierón II de Siracusa y el problema de la corona

-Marco Vitruvio (80-70 a.C, 15 d.C), ingeniero y arquitecto ("De Architectura", libro IX, §9-12)

1000 *g de oro desalojan* 51, 81 cm^3 *de agua*

1000 *g de plata desalojan* 95, 32 cm^3 *de agua*

La corona de 1000 *g desaloja* 62, 69 cm^3 *de agua*

$$d_{Au} = \frac{m_{Au}}{v_{Au}} = 19,30 \ \frac{g}{cm^3}$$

$$d_{Ag} = \frac{m_{Ag}}{v_{Ag}} = 10,49,3 \ \frac{g}{cm^3}$$

$$m_C = m_{Au} + m_{Ag} \Rightarrow m_C = d_{Au} \cdot v_{Au} + d_{Ag} \cdot v_{Ag}$$

$$v_C = v_{Au} + v_{Ag}$$

$$m_C = 1000\ g$$

$$v_C = 62,69$$

$$v_{Au} := \frac{\left(m_C - v_C \cdot 10,49\right)}{8,81} = 38,86$$

$$m_{Au} = 750\ g$$

$$m_{Ag} = 250\ g$$

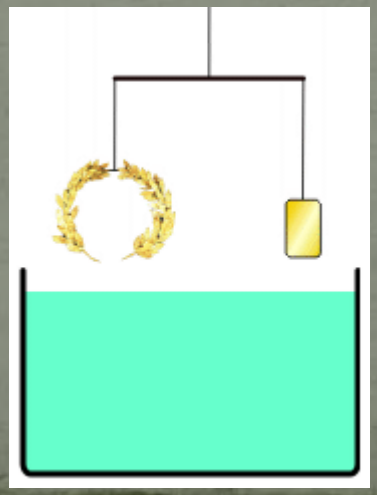
ESTOS ATAQUES NO SON TAN NOVEDOSOS EN SÍ MISMOS…

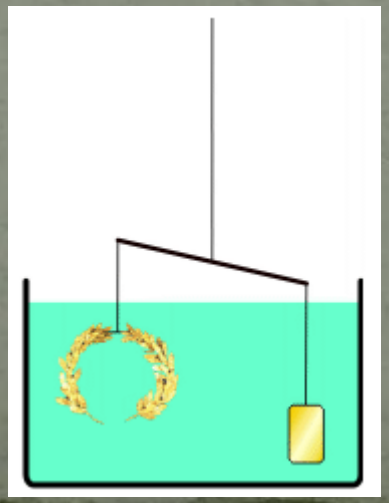
-Arquímedes, Hierón II de Siracusa y el problema de la corona

-Arquímedes (287-212 a.C)

-*"Todo cuerpo sumergido en un líquido experimenta un empuje de abajo hacia arriba igual al peso del líquido desalojado".*

-¿Falso?: Principio de Flotabilidad ("Sobre los cuerpos flotantes") y posiblemente usando una balanza, pero sin calcular la diferencia de agua desalojada (quizás).





ESTOS ATAQUES NO SON TAN NOVEDOSOS EN SÍ MISMOS…

-Reventado cajas de seguridad: esto también es cracking en dispositivos físicos.

+"Toda caja fuerte debe abrirse por un experto en caso de malfuncionamiento…. por lo tanto, puede ser abierta"

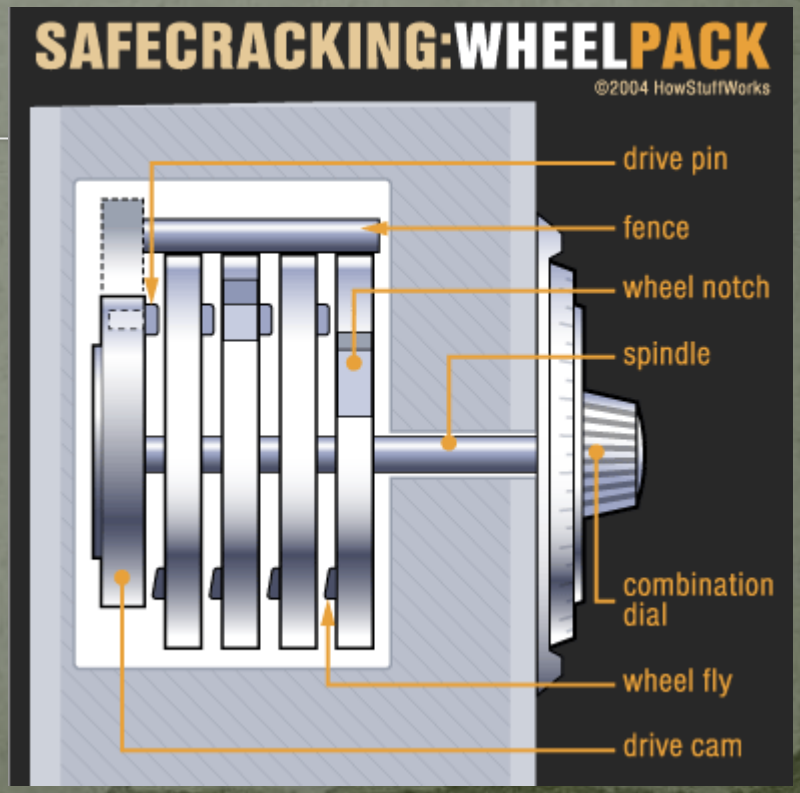
+Herramientas adecuadas + habilidad + paciencia.

+Anclajes, retardantes metálicos, de fuego,…

+Combinación :desde 1 a 3, y hasta 6 a 8.

+Mecanismo con más de 100 años en uso.

+Combinaciones habituales, por defecto, apuntadas, sólo la última…



ESTOS ATAQUES NO SON TAN NOVEDOSOS EN SÍ MISMOS...

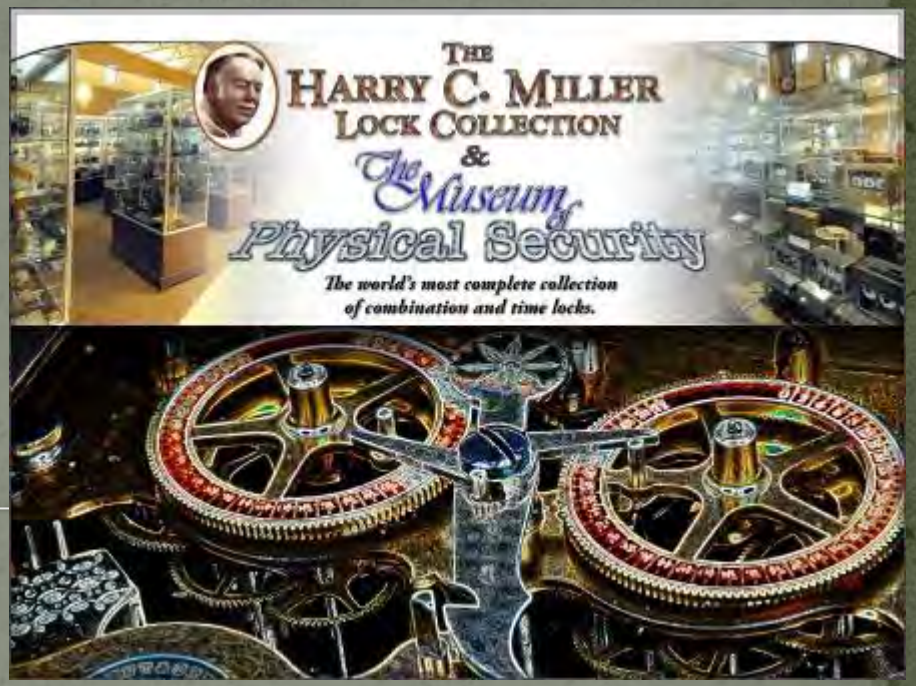
-Reventado cajas de seguridad:
esto también es cracking en dispositivos físicos.

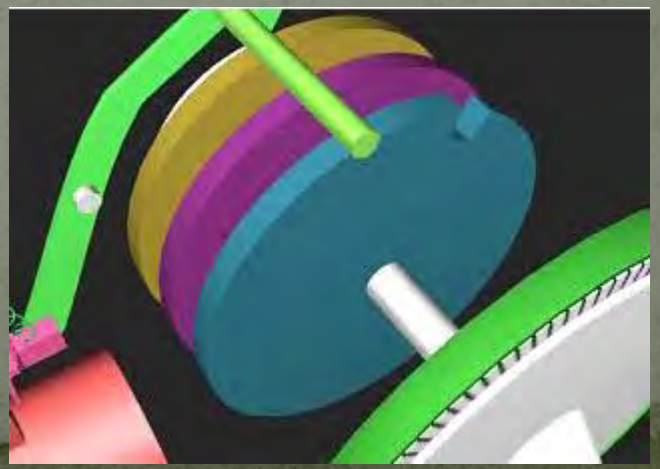
+Harry C. Miller.

+Encontrar los puntos de contacto.

+Determinar el conjunto de números (ruedas en juego).

+Buscar la correlación.

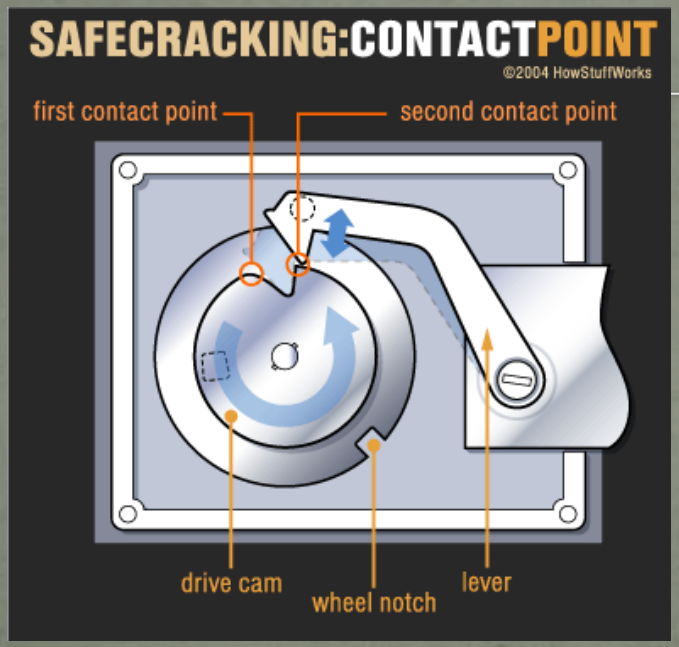




ESTOS ATAQUES NO SON TAN NOVEDOSOS EN SÍ MISMOS…

-Reventado cajas de seguridad: esto también es cracking en dispositivos físicos.

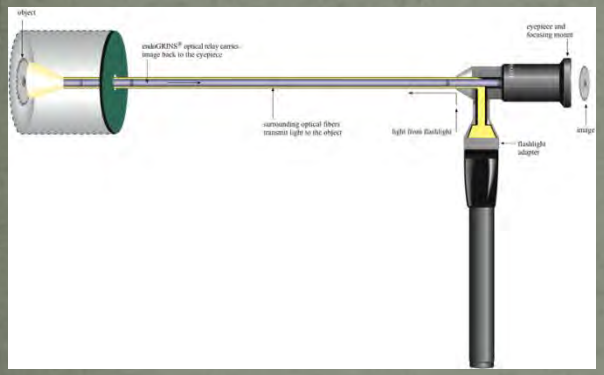
+Usando el sonido…como canal lateral: puntos de contacto, número de ruedas...

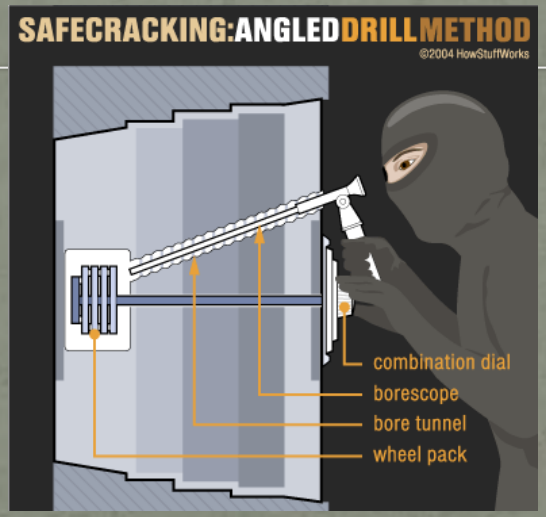


ESTOS ATAQUES NO SON TAN NOVEDOSOS EN SÍ MISMOS…

-Reventado cajas de seguridad: esto también es cracking en dispositivos físicos.

+Usando la vista…como canal lateral (borescopio): cuidado con los discos de cobalto, o las dobles cerraduras (contramedidas).





ESTOS ATAQUES NO SON TAN NOVEDOSOS EN SÍ MISMOS...

-Señal de audio en telefonía (inyección de datos).

+John T. Draper (Captain Crunch).

+Señalización "in-band".

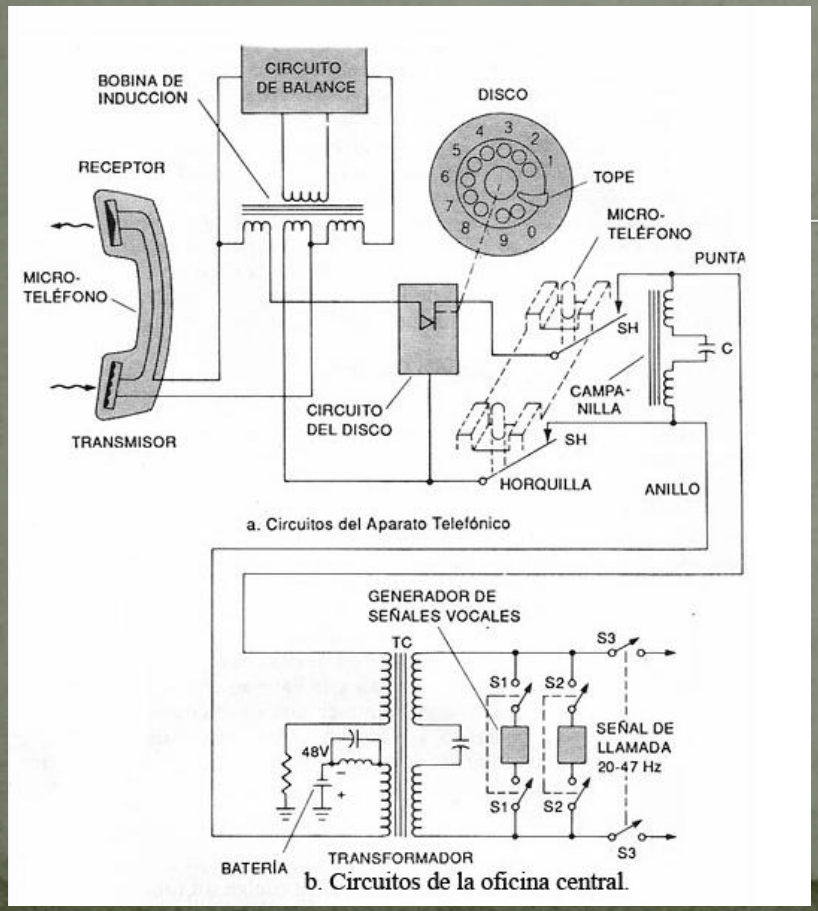
+Emitiendo a 2600 hz entrando en el sistema de señalización de la AT&T.

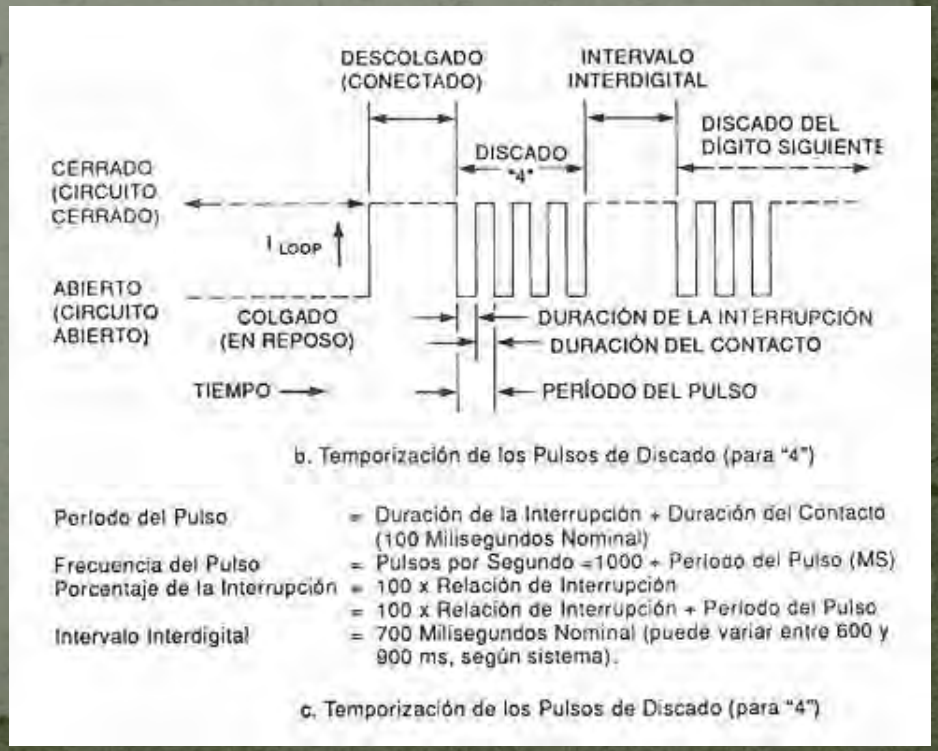
+Emitiendo a distintos tonos: blue boxes y el comienzo del phone-phreaking y el hacking.

ESTOS ATAQUES NO SON TAN NOVEDOSOS EN SÍ MISMOS...

-Ataque acústico sencillo

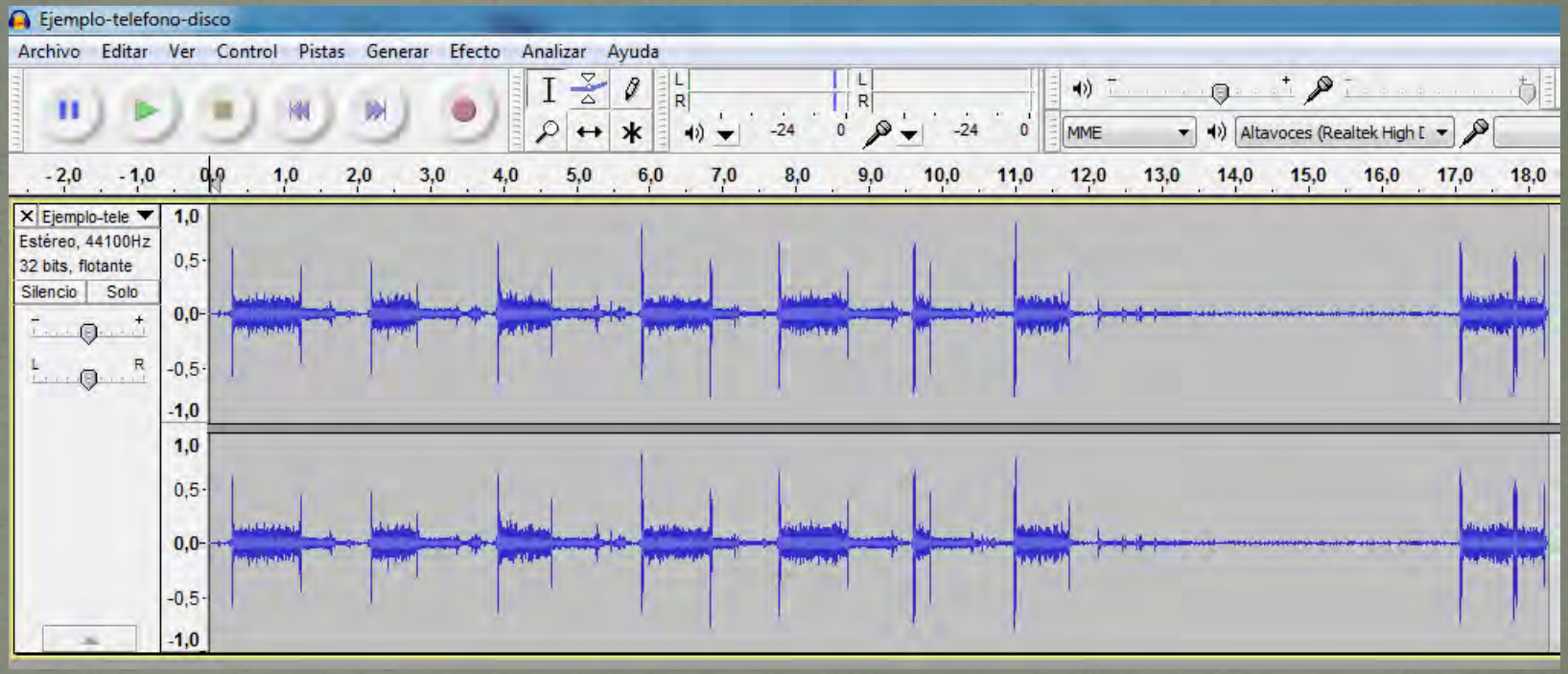
-El circuito telefónico de un modelo de marcación de décadas de disco.





ESTOS ATAQUES NO SON TAN NOVEDOSOS EN SÍ MISMOS...

-Ataque acústico sencillo



ESTOS ATAQUES NO SON TAN NOVEDOSOS EN SÍ MISMOS...

-Ataque acústico sencillo

Posición número	1º	2º	3º	4º	5º	6º	7º	8º
Duración vuelta discado (sg)	0,95	0,65	0,75	0,95	0,95	0,25	0,75	1,15

Posición número	1º	2º	3º	4º	5º	6º	7º	8º
Duración vuelta discado (sg)	0,95	0,65	0,75	0,95	0,95	0,25	0,75	1,15
Número marcado	8	5	6	8	8	1	6	0

ESTOS ATAQUES NO SON TAN NOVEDOSOS EN SÍ MISMOS...

-Ataque acústico más complicado: Operación ENGULF.

-Máquina de rotores: Hagelin.

-Boris Hagelin: criptólogo sueco (1892-1983). Uno de los constructores de máquinas de rotores criptológicas (Enigma, Purple, Hagelin, Mercury, NeMa, ...)

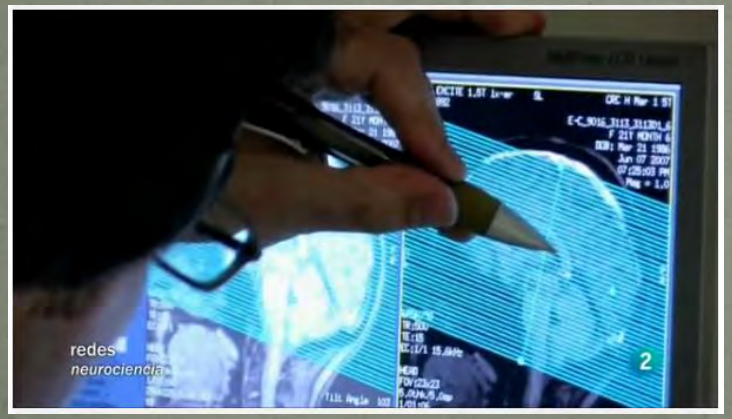
-Usada en Egipto (1956): guerra entre el coronel Gamal Abdel Nasser y los ejércitos anglo-franco-israelíes.

-Peter Wright (contraespionaje MI5) lideró el ataque acústico:
las teclas pulsadas no suenan del mismo modo.

+Desarrollado posteriormente por Dimitri Asanov y Rakesh Agrawal (2004),
y por Doug Tygar de Berkeley (2005).

...PERO PUEDEN SER SUMAMENTE FUTURISTAS Y... "DEVASTADORES"

-Ataque lateral a dispositivo físico-químico complejo y muy evolucionado.



ESTOS ATAQUES NO SON TAN NOVEDOSOS EN SÍ MISMOS…

-Esta "no-novedad" total me lleva a pensar…

…pero antes hemos de ver….

y luego ya entramos a discutir con el resto de colegas:

16:30 a 18:30	**Cómo hacer dispositivos seguros sin ser un experto en seguridad física** David Fraga, Director Estratégico, Microsoluciones en Movilidad
HORARIO	**JUEVES 12 DE JULIO**
10:00 a 12:00	**Garantías de seguridad para sistemas empotrados** Xavier Vilarrubla, IT Business Development Director, Applus+
12:00 a 12:30	CAFÉ
12:30 a 14:30	**Últimas tendencias en ataques y contramedidas** Óscar Reparaz, Investigador del centro de investigación Computer Security and Industrial Cryptography (COSIC), Katholieke Universiteit Leuven
14:30 a 16:30	COMIDA
16:30 a 18:30	**Mesa redonda: ¿Solución o mitigación? ¿Se puede evitar el éxito de este tipo de ataques?** Xavier Vilarrubla, Applus+ Óscar Reparaz, COSIC – Katholieke Universiteit Leuven Vicente Jara, CEDINT - UPM David Fraga, Microsoluciones en Movilidad José M. Moya, UPM

Material base de esta charla (en parte) [sólo nombre, título, año]:

-Algunos artículos:

-W. van Eyck, "Electromagnetic Radiation from Video Display Units: An Eavesdropping Risk?", 1985.
-P. Kocher, "Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems", 1996.
-P. Kocher, J. Jaffe, B. Jun, "Differential Power Analysis", 1998.
-P. Kocher, J. Jaffe, B. Jun, "Introduction to Differential Power Analysis and Related Attacks", 1998.
-T. Messerges, E. Dabbish, R. Sloan, "Power Analysis Attacks of Modular Exponentiation in Smartcards", 1999.
-O. Kömmerling, M. Kuhn, "Design Principles for Tamper-Resistant Smartcard Processors", 1999.
-J. Kelsey, B. Schneier, et alius, "Side Channel Cryptanalysis of Product Ciphers", 2000.
-J. R. Rao, P. Rohatgi, "EMpowering Side-Channel Attacks", 2001.
-R. Mayer-Sommer, "Smartly Analyzing the Simplicity and the Power of Simple Analysis on Smartcards", 2001.
-M. Tunstall, "Attacks on Smart Cards", 2003.
-S. Skorobogatov, R. Anderson, "Optical Fault Induction Attacks", 2003.
-X. Chen, C. Gebotys, "Simple Power Analysis Threat in Embedded Devices?", 2004.
-E. Brier, Ch. Clavier, F. Olivier, "Correlation Power Analysis with a Leakage Model", 2004.
-E. Prouff, "DPA Attacks and S-Boxes", 2005.
-L. Zhuang, F. Zhou, D. Tygar, "Keyboard Acoustic Emanations Revisited", 2005.
-B. Gierlichs, L. Batina, et alius, "Mutual Information Analysis", 2009.
-H. Douglas, "Thin Hypervisor-Based Security Architectures for Embedded Platforms", 2010.
-J. Doget, E. Prouff, et alius, "Univariate Side Channel Attacks and Leakage Modeling", 2011.
-R. Chaves, "Side Channel Analysis", 2011.
-M. Joye, F. Olivier, "Side-Channel Analysis", 2011.
-S. Skorobogatov, "Fault attacks on secure chips: from glitch to flash", 2011.

-Otro material:

-J. Verne, "Voyage au Centre de la Terre", 1864.
-Tropical Software, "DES Encryption", 1997.
-L. Goubin, J. Patarin, "DES and Differential Power Analysis. The "Duplication" Method", 1999.
-Microchip Technology, "PIC16C84", 1997.
-D. James, "Intel's 22-nm Trigate Transistors Exposed", 2012.
-SciencePhoto Library, "Scanning electron micrograph of a silicon chip", 2001.
-M. Vitruvio, "De Architectura", 1914 [traducción del autor].
-1010.co.uk/org/tempest_presn.html, "Workshop TEMPEST", 2008.
-Historiayleyenda.com, "El aparato telefónico", 2008.
-HowStuffWorks.com, "How Safecracking Works", 1998.
-H. Miller, "Harry C. Miller Lock Collection", 2008.
-J. Draper, "The Real Captain Crunch", 2007.
-Todos diversas de Wikipedia (CMOS, Arquímedes, telefonía, instrumental de microscopía, etc.)

Gracias por su atención

¿Alguna pregunta?